PARTIAL TRANSLATION OF JP 2000-132515 A

Publication Date: May 12, 2000
Title of the Invention: DEVICE AND METHOD FOR JUDGING WRONG ACCESS
Patent Application Number: 10-302008
Filing Date: October 23, 1998
Inventors: Yusaku FUJII et al.
Applicant: FUJITSU LTD.

(Page 5, left column, lines 29 – 40)
[0030] A storage part stores the position of a terminal, such as a TEL number and a network address, which is to be a transmission source, as well as ID information and information on living body input in the past. A comparison/collation part compares and collates the input ID information and information on a living body with the ID information and information on a living body input in the past through the same terminal position.

[0031] An attacker may perform round-robin attacks from a particular terminal, using forged information on a living body and information on his/her living body. In this case, it would be a big burden to conduct comparison and collation with respect to all the ID information and information on a living body input in the past. Therefore, currently, by narrowing terminals to be compared and collated for ID information and information on a living body down to a particular terminal that is being input, the burden of comparison and collation is reduced.

(Page 5, right column, lines 19 – 24)
[0037] As information on a living body used in a device for judging a wrong access, a fingerprint, a voice print, an iris pattern, a retina blood-vessel pattern, a palm shape, an ear shape, a face, a signature, and the like are used. These pieces of information on a living body are assumed to be

peculiar to a human, and assuming that information on a living body cannot be the same if ID information is different, a wrong access is determined.

(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2000132515 A**

(43) Date of publication of application: **12.05.00**

(51) Int. Cl **G06F 15/00**
G06F 1/00
G06T 7/00

(21) Application number: **10302008**

(22) Date of filing: **23.10.98**

(71) Applicant: **FUJITSU LTD**

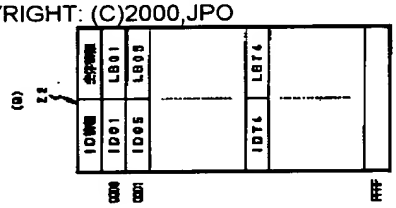
(72) Inventor: **FUJII YUSAKU**
NIIZAKI TAKU

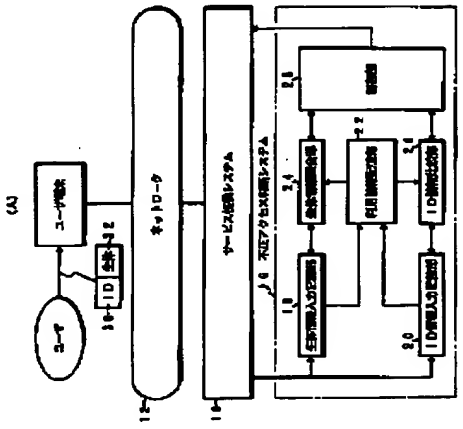
(54) DEVICE AND METHOD FOR JUDGING WRONG ACCESS

(57) Abstract:

PROBLEM TO BE SOLVED: To monitor and judge a wrong access of an attacker who pretends to be a normal user and to support a service providing system which asks for authenticating the personal identification based on an ID information and organismic information.

SOLUTION: The service providing system 10 inputs the ID information and the organismic information based on the authentication request received from a user terminal, stores these information in an application information storage part 22 and then collates the ID information and the organismic information of an ID information input storage part 20 and a organismic information input storage part 18 with the ID information and the organismic information which are inputted in the past to an application information storage part 28 via a collation part 24 and a comparison part 26. A control part 28 judges the authentication request given from a wrong accessing person based on the result of the said collation, notifies the system 10 of the wrong access and performs the logging of the identify information on the wrong accessing person.





(19)日本国特許庁(JP)　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開２０００－１３２５１５
（Ｐ２０００－１３２５１５Ａ）
(43)公開日　平成12年5月12日(2000.5.12)

(51)Int.Cl.⁷		識別記号	FI			テーマコード(参考)
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０Ｆ	5B043
	1/00	３７０		1/00	３７０Ｅ	5B085
Ｇ０６Ｔ	7/00			15/62	４６５Ａ	

審査請求　未請求　請求項の数２０　ＯＬ　(全２４頁)

(21)出願番号　特願平10-302008

(22)出願日　平成10年10月23日(1998.10.23)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中4丁目1番1号

(72)発明者　藤井　勇作
神奈川県川崎市中原区上小田中4丁目1番1号　富士通株式会社内

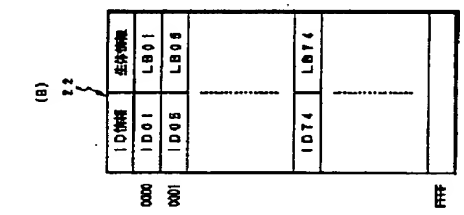
(72)発明者　新崎　卓
神奈川県川崎市中原区上小田中4丁目1番1号　富士通株式会社内

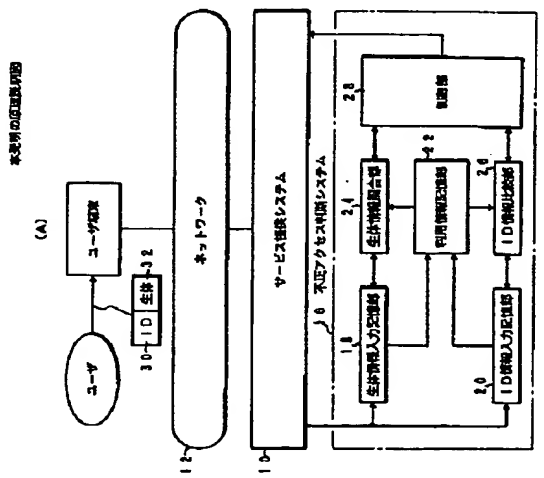
(74)代理人　100079359
弁理士　竹内　進　(外1名)

最終頁に続く

(54)【発明の名称】不正アクセス判断装置及び方法

(57)【要約】
【課題】ＩＤ情報と生体情報を使用して本人確認の認証請求行なうサービス提供システムに対する正規ユーザになりすましたアタッカの不正アクセスを監視判断して支援する。
【解決手段】サービス提供システム１０が利用者端末１４から受けた認証請求に基づくＩＤ情報及び生体情報を入力して利用情報記憶部２２に記憶し、生体情報入力記憶部１８とＩＤ情報入力記憶部２０のＩＤ情報及び生体情報と利用情報記憶部２８に過去に入力されたＩＤ情報及び生体情報とを照合部２４と比較部２６で比較照合する。制御部２８は、比較照合の結果に基づいて不正アクセス者による認証請求を判断してサービス提供システム１０に通知したり、不正アクセス者の身元情報をロギングする。





1

【特許請求の範囲】

【請求項１】サービス提供システムが利用者から受けた認証請求に基づくＩＤ情報及び生体情報を入力して記憶する記憶部と、

入力されたＩＤ情報及び生体情報と過去に入力されたＩＤ情報及び生体情報と比較照合する比較照合部と、

前記比較照合部の出力に基づき不正アクセス者による認証請求を判断して前記サービス提供システムに通知する制御部と、を設けたことを特徴とする不正アクセス判断装置。

【請求項２】請求項１記載の不正アクセス判断装置に於いて、前記記憶部は、

サービス提供システムが利用者から受けた認証請求に基づくＩＤ情報及び生体情報を入力して一時記憶する入力記憶部と、

過去にサービス提供システムが利用者から受けた認証請求に基づくＩＤ情報及び生体情報を保存記憶する利用情報記憶部と、を備えたことを特徴とする不正アクセス判断装置。

【請求項３】請求項１記載の不正アクセス判断装置に於いて、前記制御部は、前記比較照合部の出力によりＩＤ情報が不一致で生体情報が一致する場合、或いは、ＩＤ情報が一致して生体情報が不一致の場合に、不正アクセス者による認証請求と判断することを特徴とする不正アクセス判断装置。

【請求項４】請求項１記載の不正アクセス判断装置に於いて、

前記記憶部は、過去に入力したＩＤ情報及び生体情報に対応して送信元となる電話番号やネットワークアドレス等の端末位置及び入力時刻を記憶し、

前記制御部は、前記比較照合部による入力したＩＤ情報と同一端末位置から所定時間内に入力した過去のＩＤ情報と比較結果が不一致の場合、不正アクセス者による認証請求と判断することを特徴とする不正アクセス判断装置。

【請求項５】請求項１記載の不正アクセス判断装置に於いて、前記制御部は、入力したＩＤ情報に対し過去のＩＤ情報が連番になっているか否か判定し、連番を判定した際には所定回数目で不正アクセス者による認証請求と判断することを特徴とする不正アクセス判断装置。

【請求項６】請求項１記載の不正アクセス判断装置に於いて、前記制御部は、入力した生体情報と過去に入力した生体情報が一致した際に、生体情報が一致しＩＤ情報が異なる組合せを検出し、該組合せ数が所定数に達した時に、不正アクセス者による認証請求と判断することを特徴とする不正アクセス判断装置。

【請求項７】請求項１記載の不正アクセス判断装置に於いて、前記比較照合部は、

入力したＩＤ情報と過去に入力したＩＤ情報とを比較して一致又は不一致を出力するＩＤ情報比較部と、

2

入力した生体情報と過去に入力した生体情報とを比較し、所定の一致度以上の値が得られた場合に生体情報の一致を出力し、所定の一致度未満の値が得られた場合に生体情報の不一致を出力する生体情報照合部と、を備えた特徴とする不正アクセス判断装置。

【請求項８】請求項１記載の不正アクセス判断装置に於いて、更に時間を計測する時計部を設け、前記時計部で計測した時間情報に基づき、記憶されてから所定時間が経過した過去に入力したＩＤ情報及び生体情報を消去して比較照合の対象から除外することを特徴とする不正アクセス判断装置。

【請求項９】請求項１記載の不正アクセス判断装置に於いて、

前記記憶部は、過去に入力したＩＤ情報及び生体情報と共に送信元となる電話番号やネットワークアドレス等の端末位置を記憶し、

前記比較照合部は、入力したＩＤ情報及び生体情報を、同じ端末位置から過去に入力したＩＤ情報及び生体情報と比較照合することを特徴とする不正アクセス判断装置。

【請求項１０】請求項１記載の不正アクセス判断装置に於いて、更に、

端末アドレス毎に認証請求の回数を記録する認証請求端末アドレス記録部と、

前記認証請求端末アドレスの参照により所定時間内に所定回数以上の認証請求が行われたことを検知し、前記比較照合部及び制御部を起動して不正アクセスを判断させる同一端末アクセス検知部と、を設けたことを特徴とする不正アクセス判断装置。

【請求項１１】サービス提供システムが利用者から受けた認証請求に基づくＩＤ情報及び生体情報を入力して記憶する記憶過程と、

入力されたＩＤ情報及び生体情報と過去に入力されたＩＤ情報及び生体情報と比較照合する比較照合過程と、

前記比較照合過程の出力に基づいて不正アクセス者による認証請求を判断して前記サービス提供システムに通知する制御過程と、を設けたことを特徴とする不正アクセス判断方法。

【請求項１２】請求項１１記載の不正アクセス判断方法に於いて、前記記憶過程は、

サービス提供システムが利用者から受けた認証請求に基づくＩＤ情報及び生体情報を入力して一時記憶する入力記憶過程と、

過去にサービス提供システムが利用者から受けた認証請求に基づくＩＤ情報及び生体情報を保存記憶する利用情報記憶過程と、を備えたことを特徴とする不正アクセス判断方法。

【請求項１３】請求項１１記載の不正アクセス判断方法に於いて、前記制御過程は、前記比較照合過程の出力によりＩＤ情報が不一致で生体情報が一致する場合、或い

は、ＩＤ情報が一致して生体情報が不一致の場合に、不正アクセス者による認証請求と判断することを特徴とする不正アクセス判断方法。

【請求項１４】請求項１１記載の不正アクセス判断方法に於いて、

前記記憶過程は、過去に入力したＩＤ情報及び生体情報に対応して送信元となる電話番号やネットワークアドレス等の端末位置及び入力時刻を記憶し、

前記制御過程は、前記比較照合過程による入力したＩＤ情報と同一端末位置から所定時間内に入力した過去のＩＤ情報と比較結果が不一致の場合、不正アクセス者による認証請求と判断することを特徴とする不正アクセス判断方法。

【請求項１５】請求項１１記載の不正アクセス判断方法に於いて、前記制御過程は、入力したＩＤ情報に対し過去のＩＤ情報が連番になっているか否か判定し、連番を判定した際には所定回数目で不正アクセス者による認証請求と判断することを特徴とする不正アクセス判断方法。

【請求項１６】請求項１１記載の不正アクセス判断方法に於いて、前記制御過程は、入力した生体情報と過去に入力した生体情報が一致した際に、生体情報が一致しＩＤ情報が異なる組み合せを検出し、該組み合せ数が所定数に達した時に、不正アクセス者による認証請求と判断することを特徴とする不正アクセス判断方法。

【請求項１７】請求項１１記載の不正アクセス判断方法に於いて、前記比較照合過程は、

入力したＩＤ情報と過去に入力したＩＤ情報とを比較して一致又は不一致を出力するＩＤ情報比較過程と、

入力した生体情報と過去に入力した生体情報とを比較し、所定の一致度以上の値が得られた場合に生体情報の一致を出力し、所定の一致度未満の値が得られた場合に生体情報の不一致を出力する生体情報照合過程と、を備えたことを特徴とする不正アクセス判断方法。

【請求項１８】請求項１１記載の不正アクセス判断方法に於いて、更に時間を計測する時計過程を設け、前記時計過程で計測した時間情報に基づき、記憶されてから所定時間が経過した過去に入力したＩＤ情報及び生体情報を消去して比較照合の対象から除外することを特徴とする不正アクセス判断方法。

【請求項１９】請求項１１記載の不正アクセス判断方法に於いて、

前記記憶過程は、過去に入力したＩＤ情報及び生体情報と共に送信元となる電話番号やネットワークアドレス等の端末位置を記憶し、

前記比較照合過程は、入力したＩＤ情報及び生体情報を、同じ端末位置から過去に入力したＩＤ情報及び生体情報と比較照合することを特徴とする不正アクセス判断方法。

【請求項２０】請求項１１記載の不正アクセス判断方法に於いて、更に、

端末アドレス毎に認証請求の回数を記録する認証請求端末アドレス記録過程と、　前記認証請求端末アドレスの参照により所定時間内に所定回数以上の認証請求が行われたことを検知し、前記比較照合過程及び制御過程を起動して不正アクセスを判断させる同一端末アクセス検知過程と、を設けたことを特徴とする不正アクセス判断方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、サービス提供システムに対するアタッカの不正なアクセスを判断する不正アクセス判断装置及び方法に関し、特に、ＩＤ情報に指紋や虹彩等の生体情報を組み合わせてサービス提供システムに認証請求を行う際のアタッカの不正アクセスを判断する不正アクセス判断装置及び方法に関する。

【０００２】

【従来の技術】現在、通信回線のインフラが整いつつあり、コンピュータなどの情報機器が通信回線を介して相互に接続され、利用者は、遠隔地から様々なサービスを利用できるようになっいる。

【０００３】このようなサービス提供システムでは、システム利用時、利用者が正規ユーザであるかどうかをパスワードを用いて確かめている。また近年では、指紋や虹彩などの生体情報を用いて、本人確認する技術が確立しつつあり、本人確認にこれらの生体情報照合を応用することが考えられる。

【０００４】

【発明が解決しようとする課題】しかしながら、このようなサービス提供システムにあっては、正規のユーザ以外に、悪意のある者が手軽に遠隔地から各種の情報機器に不正にアタックできる可能性がある。例えば、遠隔地から自分のコンピュータを使って自動的にパスワードを発見するプログラムを作成できるため、犯罪者にとっても犯罪しやすい環境が整いつつある。

【０００５】そこでシステムの利用するための認証請求に対する本人確認のため、ＩＤコードに指紋や虹彩などの生体情報を組み合わせてセキュリティを高めているが、正規ユーザの生体情報を不正に入手できれば、ＩＤコードを変えながら生体情報を連続入力するといった手法でアタックされる可能性がある。

【０００６】このため生体情報を個人認証に使用した場合にも、ますます、犯罪者からのアタックを意識したシステムを構築する必要がある。

【０００７】本発明は、認証請求にＩＤ情報と生体情報を使用したサービス提供システムに対し、正規ユーザになりすました不正アクセス者のアタックを監視判断してシステムを支援する不正アクセス判断装置及び方法を提供することを目的とする。

【０００８】

【課題を解決するための手段】図１は本発明の原理説明図である。

【０００９】本発明は、図１（Ａ）のように、サービス提供システム１０が利用者端末１４から受けた認証請求に基づくＩＤ情報３０及び生体情報３２を入力して記憶する記憶部、記憶部に入力されたＩＤ情報及び生体情報と過去に入力されたＩＤ情報及び生体情報と比較照合する比較照合部、及び比較照合部の出力に基づいて不正アクセス者による認証請求を判断してサービス提供システム１０に通知する制御部２８とを設けたことを特徴とする。

【００１０】このように本発明は、ユーザがＩＤ情報と生体情報を用いてシステムに対し本人確認のための認証請求を行った際に、保存している過去に行われた認証要求のＩＤ情報と生体情報と比べ、アタッカによる不正なアクセスかどうかを推測判断することを基本とする。もし不正にシステムに侵入しようとしているアタッカからの攻撃の可能性があると判断した場合には、サービス提供システムに不正アクセスであることを通知し、サービス提供を拒否させることで侵入を防ぐ。

【００１１】ここで記憶部は、サービス提供システムが利用者から受けた認証請求に基づくＩＤ情報及び生体情報を入力して一時記憶する入力記憶部１８，２０と、図１（Ｂ）のように、過去にサービス提供システムが利用者から受けた認証請求に基づくＩＤ情報及び生体情報を保存記憶する利用情報記憶部２２を備える。

【００１２】具体的に、アタッカの攻撃は、自分の生体情報や偽造した生体情報を使用し、これにＩＤ情報をランダムに組み合わせて認証請求を次々と発信してシステムに侵入しようとする。このためアタックの形態は、次の３つに分類できる。

【００１３】アタック形態１：生体情報を固定し、ＩＤ情報を次々と変えてアタックする。

【００１４】アタック形態２：ＩＤ情報を固定し、生体情報を次々と変えてアタックする。

【００１５】アタック形態２：③生体情報とＩＤ情報の両方を次々と変えてアタックする。

【００１６】本発明の制御部２８は、これらアタック形態に対応する不正アクセスの判断ルールとして次のものを備える。

【００１７】［判断ルール１］制御部２８は、比較照合部の出力によりＩＤ情報が不一致で生体情報が一致している場合に、不正アクセス者による認証請求と判断する。これは、アタック形態１であり、アタッカが偽造した生体情報や自分の生体情報を使用し、複数利用者のＩＤ情報に組み合わせて認証請求を行った場合である。例えば生体情報に指紋を用いている場合には、アタッカは、利用者のＩＤ番号を入力し、指を指紋スキャナに押すという動作を繰り返している。

【００１８】［判断ルール２］制御部２８は、比較照合部の出力によりＩＤ情報が一致して生体情報が不一致の場合に、不正アクセス者による認証請求と判断する。これはアタック形態２であり、アタッカが偽造した生体情報や自分の生体情報を使用し、特定のＩＤ情報に組み合わせて認証請求を行った場合である。例えば生体情報に指紋を用いている場合には、アタッカは、同一のＩＤ番号を入力し、指を変えながら指紋スキャナに押すという動作を繰り返している。

【００１９】［判断ルール３］制御部２８は、比較照合部の出力によりＩＤ情報が不一致で生体情報が一致する場合、或いは、ＩＤ情報が一致して生体情報が不一致の場合に、不正アクセス者による認証請求と判断する。これはアタック形態３であり、アタッカが偽造した生体情報や自分の生体情報を使用し、複数利用者のＩＤ情報に組み合わせて認証請求を行った場合である。例えば生体情報に指紋を用いている場合には、アタッカは、指を変えながら指紋スキャナに押すという動作を、利用者のＩＤ番号を変えながら繰り返している。

【００２０】［判断ルール４］記憶部は、過去に入力したＩＤ情報及び生体情報に対応して、送信元となる電話番号やネットワークアドレス等の端末位置及び入力時刻を記憶し、制御部は、同一端末から新たに入力したＩＤ情報と、過去の所定時間内に同一端末から入力されたＩＤ情報と比較した結果が不一致の場合、不正アクセス者による認証要求と判断する。

【００２１】これはアタックは通常コンピュータを用いて、自動的に大量の認証請求を集中して行うことに着目したものであり、過去に入力した生体情報との照合を行わずに不正使用の判断ができる。

【００２２】［判断ルール５］制御部２８は、入力したＩＤ情報に対し過去のＩＤ情報が連番になっているか否か判定し、連番を判定した際には所定回数目で不正アクセス者による認証請求と判断する。

【００２３】利用者のＩＤ情報が連番で続けて入力されている場合は、一層アタッカからの攻撃の可能性が高い。アタッカがコンピュータを使って順番に攻撃していることが考えられるからである。したがって、入力されるＩＤが連番であるかどうか調べると、アタッカからの攻撃であることの確信が持て、不正アクセスかどうかの確からしさが向上する。

【００２４】［判断ルール６］制御部２８は、入力した生体情報と過去に入力した生体情報が一致した際に、生体情報が一致しＩＤ情報が異なる組合せを検出し、この組合せ数が所定数に達した時に、不正アクセス者による認証請求と判断する。

【００２５】一方、アタッカが不正にアクセスしようとしたのではなく、正規の利用者が単にＩＤ情報を入力し間違える場合もある。そこで所定の回数、例えば３回まではＩＤ情報を再入力できるようにし、ＩＤ情報の入力し間違いを不正アクセスと誤認することを回避する。

【００２６】比較照合部は、入力したＩＤ情報と過去に入力したＩＤ情報とを比較して一致又は不一致を出力するＩＤ情報比較部２４と、入力した生体情報と過去に入力した生体情報とを比較し、所定の一致度以上の値が得られた場合に生体情報の一致を出力し、所定の一致度未満の値が得られた場合に生体情報の不一致を出力する生体情報照合部２６とで、ＩＤ情報と生体情報の比較照合を個別にできるようにしている。

【００２７】本発明の不正アクセス判断装置は、更に時間を計測する時計部を設け、時計部で計測した時間情報に基づき、記憶されてから所定時間が経過した過去に入力したＩＤ情報及び生体情報を消去して比較照合の対象から除外する。

【００２８】正規のユーザが不正にアクセスしようとしたのではなく、単にＩＤ情報を入力し間違える場合、いつまでもその事実を保存記憶しておくと、正規のユーザ本人であるにも関わらず、不正アクセスと判定されてアクセスできない状況が発生し得る。そこで、記憶保存に時間制限を行って所定時間が経過したら消去し、不正アクセスと誤認される状況を回避する。

【００２９】一般的にアタッカは、短時間に集中的に攻撃を行うので、保存記憶に時間制限を行ってもアタッカの不正アクセスを判断するための保存記憶は十分に得られる。このため正規のユーザが何回もＩＤ情報を入力し間違えても、システムを利用できる。更に、保存記憶の時間が制限されることで、過去に入力したＩＤ情報及び生体情報の記憶量が制限され、新たに入力したＩＤ情報及び生体情報との照合比較の負担が低減する。

【００３０】記憶部は、過去に入力したＩＤ情報及び生体情報と共に送信元となる電話番号やネットワークアドレス等の端末位置を記憶し、比較照合部は、入力したＩＤ情報及び生体情報を、同じ端末位置から過去に入力したＩＤ情報及び生体情報と比較照合する。

【００３１】アタッカは偽造した生体情報や自分の生体情報を用いて、特定の端末から総当たり攻撃を行ってくる場合がある。この場合、過去に入力されたＩＤ情報及び生体情報の全てと比較照合することは大きな負担になる。そこで、ＩＤ情報と生体情報の比較照合を行う端末を、現在、入力を行っている特定の端末に絞ることで、比較照合の負担を減らす。

【００３２】本発明の不正アクセス判断装置は、更に、不正アクセス者の情報を記録するログ記録部を設ける。ログ記録部には、不正アクセス者の生体情報、不正アクセス者の電話番号もしくはネットワークアドレス等の端末位置、及び不正アクセスの対象となったＩＤ情報の少なくともいずれかを記録する。

【００３３】ＩＤ情報に比べ生体情報は、盗むことが困難であることを考えると、用いられた生体情報はアタッカのものである確率が高く、これをロギングすることで犯罪装置の手掛かりとでき、不正アクセス者の特定や証拠に活用できる。

【００３４】また端末の位置や時間等を保存しておくことで、犯罪捜査の手掛かりとなる他、アタッカからの攻撃時にログ記録部を参照して端末を積極的に調べることができる。更に攻撃対象となったＩＤ情報の記録保存により、再攻撃に対してのセキュリティ対策に役立てることができる。

【００３５】本発明の不正アクセス判断装置は、更に、端末アドレス毎に認証請求の回数を記録する認証請求端末アドレス記録部と、認証請求端末アドレスの参照により所定時間内に所定回数以上の認証請求が行われたことを検知し、比較照合部及び制御部を起動して不正アクセスを判断させる同一端末アクセス検知部とを設ける。

【００３６】これは通常の業務では考えられないような同一端末からの認証請求の回数を検知した場合にのみ、ＩＤ情報と生体情報の比較照合に基づく不正アクセスの判断を起動するもので、不正判断の処理負担を減らすことができる。

【００３７】不正アクセス判断装置で使用する生体情報としては、指紋、声紋、虹彩パターン、網膜血管パターン、掌形、耳形、顔、署名等を用いる。これらの生体情報は人に固有のものと仮定でき、ＩＤ情報が異なるのにも関わらず生体情報が同じであるということは発生しないと仮定して不正アクセスを判断する。

【００３８】制御部２８は、不正アクセス者による認証請求を判断した際に、サービス提供システム１０の管理者に判断結果を自動通知する。制御部２８による管理者への自動通知は、固定電話、携帯電話、電子メール、専用通信回線、警告灯などを用いて通知する。

【００３９】アタッカからの攻撃であると判断された場合、その事実をシステム側からシステム管理者側に通知することで、システム管理者は、常にシステムを監視している必要はなく、管理者側の管理負担が軽減される。自動通知には広く普及している電話や電子メールを用いることで、コストが削減できる。

【００４０】更に、本発明は不正アクセス判断方法を提供するものであり、サービス提供システムが利用者から受けた認証請求に基づくＩＤ情報及び生体情報を入力して記憶する記憶過程；入力されたＩＤ情報及び生体情報と過去に入力されたＩＤ情報及び生体情報と比較照合する比較照合過程；前記比較照合過程の出力に基づいて不正アクセス者による認証請求を判断して前記サービス提供システムに通知する判断制御過程；を備える。この不正アクセス判断方法の詳細は、装置構成と基本的に同じになる。

【００４１】

【発明の実施の形態】図２は、本発明の不正アクセス判断装置の第１実施形態のブロック図である。

【００４２】図２において、本発明による不正アクセスの判断対象となるサービス提供システム１０は、例えば

インターネットやイントラネット等のネットワーク１２を介してユーザ端末１４からのサービス要求を受け、ユーザが要求したサービスをオンラインで提供している。

【００４３】このようなサービス提供システム１０はオンライン検索機能を備えたデータベースシステム等の適宜のサービスを提供するシステムであり、例えば百万人を越える膨大な数の正規ユーザが利用するシステム等である。

【００４４】このサービス提供システム１０をユーザがユーザ端末１４からのアクセスで利用する場合には、ユーザはサービス提供システム１０側に予め登録されたＩＤ情報３０とユーザに固有の生体情報（ＬＢ情報）３２を入力し、ユーザ端末１４からネットワーク１２を経由してサービス提供システム１０に対し正規ユーザであることを確認するための認証請求（本人確認の認証請求）を行う。

【００４５】この実施例において、ユーザが入力する生体情報３２としては指紋を例に説明するが、これ以外に虹彩、声紋、網膜血管分布、署名等の生体情報を用いることができる。また生体情報の種類は、サービス提供システム１０側に設けられている生体情報照合システムによって異なるが、例えば指紋なら指紋画像や指紋画像から抽出された生体キー情報を用いる。

【００４６】正規のユーザのＩＤ情報３０及び生体情報３２は、ユーザがサービス提供システム１０の利用申込みを行った際に、サービス提供システム１０側に予め登録されている。このため、ユーザがＩＤ情報３０と生体情報３２を入力してユーザ端末１４からサービス提供システム１０に対し認証請求を行うと、サービス提供システム１０側において認証請求のあったＩＤ情報３０に対応して予め登録している生体情報３２を読み出し、入力した生体情報３２と登録済みの生体情報を照合し、所定値以上の一致度が得られたときに生体情報は同じもの（照合一致）とし、認証請求のあったユーザ端末１４に対しサービス提供システム１０の利用を許可する。

【００４７】このような認証請求にＩＤ情報３０と生体情報３２の組合せを用いたサービス提供システム１０に対し、アタッカによる不正アクセスを判断するため、本発明の不正アクセス判断システム１６が支援装置として設けられている。不正アクセス判断システム１６は、生体情報入力記憶部１８、ＩＤ情報入力記憶部２０、利用情報記憶部２２、生体情報照合部２４、ＩＤ情報比較部２６及び制御部２８で構成される。

【００４８】生体情報入力記憶部１８とＩＤ情報入力記憶部２０には、サービス提供システム１０に対しユーザ端末１４よりＩＤ情報３０と生体情報３２を使用した認証請求があった際に、サービス提供システム１０に入力された生体情報３２及びＩＤ情報３０のそれぞれを一時的に入力記憶する。

【００４９】利用情報記憶部２２には、サービス提供システム１０に対するユーザ端末１４からの認証請求で過去に入力されたＩＤ情報と生体情報がペアで記憶保存されている。

【００５０】図３は図２の利用情報記憶部２２の記憶内容である。利用情報記憶部２２は、ＩＤ情報記憶領域２２－１と生体情報記憶領域２２－２をもち、ＩＤ情報と生体情報をペアにして例えば（ＩＤ０１，ＬＢ０１）（ＩＤ０５，ＬＢ０５），・・・のように保存記憶している。利用情報記憶部２２の記憶領域は、例えば１６進のアドレス０００００～ＦＦＦＦで決まるメモリ容量を持っており、このため最新に入力されたＩＤ情報と生体情報のペアを物理的なメモリ容量で決まる固定数分だけ記憶することになる。

【００５１】再び図２を参照するに、生体情報照合部２４は、生体情報入力記憶部１８に生体情報の入力記憶があったとき、利用情報記憶部２２に保存記憶している過去に入力した生体情報との照合を行う。この生体情報の照合は、入力した生体情報と過去に入力した生体情報との一致度を求め、一致度が所定値以上であれば照合一致の出力を生じ、一致度が所定値未満であれば照合不一致の出力を生ずる。

【００５２】ＩＤ情報比較部２６は、ＩＤ情報入力記憶部２０にＩＤ情報が入力されると、利用情報記憶部２２に保存記憶している過去に入力したＩＤ情報との比較を行い、一致または不一致の比較出力を生ずる。

【００５３】この生体情報照合部２４とＩＤ情報比較部２６による生体情報及びＩＤ情報の照合比較の処理は、サービス提供システム１０に対するユーザ端末１４からのＩＤ情報と生体情報の入力に基づくことから、同時に照合比較の処理動作が行われる。

【００５４】制御部２８は、生体情報照合部２４の照合結果とＩＤ情報比較部２６の比較結果を受け取り、アタッカからの攻撃による不正アクセスかどうかを判断し、判断結果をサービス提供システム１０に通知する。

【００５５】制御部２８による不正アクセスの判断は、
①判断ルール１
比較照合結果に基づき、ＩＤ情報が不一致で生体情報が一致している場合に、不正アクセス者による認証請求と判断；
②判断ルール２
比較照合結果によりＩＤ情報が一致して生体情報が不一致の場合に不正アクセス者による認証請求と判断；
③判断ルール３
比較照合結果によりＩＤ情報が不一致で生体情報が一致する場合、あるいはＩＤ情報が一致して生体情報が不一致の場合に、不正アクセス者による認証請求と判断；の３つが基本的にある。

【００５６】図４は、判断ルール１に従って制御部２８が判断する不正アクセスとそのときの利用情報記憶部２２の記憶内容である。図４の不正アクセス２５－１は、

11

アタッカが自分自身の指紋あるいは偽造した指紋による１つの生体情報ＬＢ１を使ってＩＤ情報をＩＤ１，ＩＤ２，ＩＤ３，ＩＤ４と変えながらアタックした場合である。具体的には、アタッカは正規ユーザのＩＤ番号を入力し、指を指紋スキャナに押す動作を繰り返している。

【００５７】このような不正アクセス２５－１のアタッカによる不正な認証請求に対し、本発明の不正アクセス判断システム１６の利用情報記憶部２２には、不正アクセス２５－１の入力時刻ｔ１～ｔ４に対応して、入力したＩＤ情報と生体情報のペア（ＩＤ１，ＬＢ１）（ＩＤ２，ＬＢ１）（ＩＤ３，ＬＢ１）（ＩＤ４，ＬＢ１）が保存記憶される。

【００５８】ここでアタッカによる不正アクセス２５－１は、時刻ｔ１～ｔ４のように連続的に行われるが、その間に他の正規ユーザからの認証請求も受け付けることから、利用情報記憶部２２には不正アクセス２５－１に対応した保存記憶が図示のように離散的に行われることになる。

【００５９】このようなアタッカが１つの生体情報に複数のＩＤ情報を組み合わせて不正な認証請求を行った場合、本発明の制御部２８にあっては判断ルール１を適用する。判断ルール１は比較照合結果に基づき、ＩＤ情報が不一致で生体情報が一致している場合に、不正アクセス者による認証請求と判断する。この判断ルール１による図４の不正アクセス２５－１に対する判断処理は次のようになる。

【００６０】まず時刻ｔ１の最初の不正アクセスの入力ペア（ＩＤ１，ＬＢ１）については、利用情報記憶部２２の記憶保存ペアとの比較照合を行っても、該当するペアがないことからＩＤ情報及び生体情報の両方が不一致となる。

【００６１】次に時刻ｔ２で２回目の不正アクセスによる入力ペア（ＩＤ２，ＬＢ１）が入力すると、このとき時刻ｔ１の不正入力したペア（ＩＤ１，ＬＢ１）は利用情報記憶部２２に既に保存記憶されているため、時刻ｔ２で入力した不正入力ペアと時刻ｔ１で入力して既に保存している保存ペアとの比較照合により、ＩＤ情報が不一致で生体情報が一致して判断ルール１の条件が成立する。

【００６２】したがって、時刻ｔ２で不正アクセスによるペア（ＩＤ２，ＬＢ１）が入力した時点で、本発明の制御部２８は判断ルール１に従って不正アクセス者による認証請求と判断する。

【００６３】また時刻ｔ３の不正アクセスのペア（ＩＤ３，ＬＢ１）の入力については、利用情報記憶部２２に時刻ｔ１，ｔ２で保存した２つの保存ペア（ＩＤ１，ＬＢ１）（ＩＤ２，ＬＢ１）との間で、ＩＤ情報が不一致で生体情報が一致する判断ルール１の条件が成立し、２回分の不正アクセスが判断できる。

【００６４】更に時刻ｔ４の不正アクセスによるペア

12

（ＩＤ４，ＬＢ１）の入力については、利用情報記憶部２２の過去に入力した時刻ｔ１～ｔ３の３つの保存ペアとの間の比較照合で３回分の不正アクセス者による認証請求が判断される。

【００６５】図５は、図２の制御部２８による判断ルール２が適用される不正アクセスとそのときの利用情報記憶部２２の内容である。判断ルール２は、比較照合結果によりＩＤ情報が一致して生体情報が不一致の場合に不正アクセス者による認証請求と判断する。

【００６６】この判断ルール２は、アタッカが偽造した生体情報や自分の生体情報を使用し、特定のＩＤ情報に組み合わせて認証請求を行った場合を想定している。例えば、図５の不正アクセス２５－２のように、アタッカが特定のＩＤ情報としてＩＤ１を使用し、これにアタッカが自分の生体情報や偽造した生体情報ＬＢ１，ＬＢ２，ＬＢ３，ＬＢ４を組み合わせて認証請求を行った場合である。具体的には、アタッカは同一のＩＤ番号を入力し、指を変えながら指紋スキャナを押すというような動作を繰り返している。

【００６７】このようにアタッカがＩＤ情報を固定で生体情報を変えながら認証請求を行う不正アクセス２５－２があると、これに対応して利用情報記憶部２２には離散的に不正アクセスの入力ペアが保存記憶される。

【００６８】このような不正アクセス２５－２について、判断ルール２による不正アクセスの判断は次のようになる。まず最初の時刻ｔ１の不正アクセスのペア（ＩＤ１，ＬＢ１）の入力にあっては、利用情報記憶部２２には不正アクセスに対応する保存ペアはないため、ＩＤ情報及び生体情報の両方について比較照合結果が不一致となり、判断ルール２による不正アクセスは判断できない。

【００６９】次に時刻ｔ２で不正アクセス２５－２によるペア（ＩＤ１，ＬＢ２）が入力すると、このとき利用情報記憶部２２には時刻ｔ１に入力して保存された保存ペア（ＩＤ１，ＬＢ１）があるため、両者の比較照合によりＩＤ情報が一致して生体情報が不一致となる判断ルール２の条件が成立し、不正アクセス者による認証請求と判断する。

【００７０】不正アクセス２５－２の時刻ｔ３，ｔ４についても、それ以前に不正アクセスによる保存ペアがあることから、同様に判断ルール２に従って不正アクセス者による認証請求と判断し、時刻ｔ３の場合は不正アクセスの判断回数が２回分、時刻ｔ４にあっては３回分となる。

【００７１】図６は、図２の制御部２８で不正アクセスを判断する判断ルール３の対象となる不正アクセスとそのときの利用情報記憶部２２の説明図である。判断ルール３は、図４の判断ルール４と図５の判断ルール２が想定している不正アクセスが混在した場合に対応する。即ち判断ルール３は、比較照合結果によりＩＤ情報が不一

致で生体情報が一致する場合、あるいはＩＤ情報が一致して生体情報が不一致の場合に、不正アクセス者による認証請求と判断する。

【００７２】図６の不正アクセス２５－３は、アタッカが複数のＩＤ情報としてＩＤ１，ＩＤ２，ＩＤ３の例えば３つを準備し、更に生体情報として自分の指紋や偽造した指紋ＬＢ１，ＬＢ２，ＬＢ３の３つを準備し、これらを組み合わせたペアを使って時刻ｔ１～ｔ９のように認証請求を行うアタックを行った場合である。

【００７３】このような不正アクセス２５－３による認証請求の入力ペアがあった場合の判断ルール３による不正アクセスの判断は、次のようになる。

【００７４】まず時刻ｔ１～ｔ３の不正アクセス２５－３のペア（ＩＤ１，ＬＢ１）（ＩＤ２，ＬＢ２）（ＩＤ３，ＬＢ３）にあっては、それぞれの入力時点での利用情報記憶部２２の保存ペアとの比較ではＩＤ情報及び生体情報の両方について不一致となり、既に説明した判断ルール１，２はもちろんのこと、この場合の判断ルール３による不正アクセスも判断できない。

【００７５】次に時刻ｔ４で、既に使用したが異なる組合せのペア（ＩＤ１，ＬＢ３）を不正アクセスで入力すると、このとき利用情報記憶部２２に記憶している時刻ｔ３の保存ペア（ＩＤ３，ＬＢ３）と時刻ｔ４の入力ペア（ＩＤ１，ＬＢ３）との間で、既に説明した判断ルール１の「ＩＤ情報が不一致で生体情報が一致する」の条件が成立し、不正アクセス者による認証請求と判断できる。

【００７６】同時に時刻ｔ１の保存ペア（ＩＤ１，ＬＢ１）と時刻ｔ４の入力ペア（ＩＤ１，ＬＢ３）との間で、既に説明した判断ルール２の「ＩＤ情報が一致して生体情報が不一致」とする条件が成立し、同様に不正アクセス者による認証請求と判断できる。

【００７７】このように判断ルール３にあっては、不正アクセス２５－３のようなＩＤ情報と生体情報の両方を変えながらアタッカが不正な認証請求を行った場合、ある入力時点で判断ルール１と判断ルール２の両方による不正アクセスの判断結果が同時に得られる。

【００７８】この点は時刻ｔ５，ｔ６の不正アクセスの入力ペアについても同様である。更に時刻ｔ７～ｔ９の不正アクセスの入力ペアについては、利用情報記憶部２２の時刻ｔ１～ｔ３と時刻ｔ４～ｔ６の中に２個ずつ同じＩＤ情報と生体情報が存在することから、例えば時刻ｔ２の不正アクセスによる入力ペア（ＩＤ１，ＬＢ２）については、判断ルール１と判断ルール２の各々による２回分の不正アクセスの判断結果が得られ、このため合計４つの不正アクセスの判断結果が同時に得られる。この点は時刻ｔ８，ｔ９の不正アクセスの入力ペアについても同様である。

【００７９】ここで制御部２８による３種類の不正アクセスに対する判断ルール１～３の使い方としては、生体情報が偽造しにくい場合についてはアタッカは同じ生体情報を使ってＩＤ情報を変えてくることから、判断ルール１を使用すればよい。

【００８０】これに対し比較的偽造が容易な生体情報の場合については、ＩＤ情報が一致して生体情報が不一致の場合に不正アクセスと判断する判断ルール２を適用すればよい。もちろん最も強力な判断ルールは、ＩＤ情報及び生体情報の両方を変えてくる場合に対応した判断ルール３である。

【００８１】図７は、図２の不正アクセス判断システム１６の第１実施形態における不正アクセス判断処理のフローチャートであり、制御部２８の判断ルールとしては図６に示した判断ルール３を適用している。

【００８２】図７において、まずステップＳ１でサービス提供システム１０に対するユーザ端末からの認証請求があると、この認証請求に伴って受信されたＩＤ情報と生体情報がステップＳ１で取得され、生体情報入力記憶部１８及びＩＤ情報入力記憶部２０のそれぞれに記憶される。

【００８３】続いてステップＳ２で、入力記憶した生体情報と利用情報記憶部２２に記憶保存している全ての生体情報を照合する。次にステップＳ３で、入力記憶したＩＤ情報と利用情報記憶部２２に記憶保存している全てのＩＤ情報を比較する。このステップＳ２，Ｓ３の生体情報の照合及びＩＤ情報の比較による結果は制御部２８に通知され、ステップＳ４，Ｓ５で判断ルール３に従った比較照合結果の判定が行われる。

【００８４】まずステップＳ４は判断ルール１による判定であり、生体情報が一致しＩＤ情報の異なるものかどうかチェックする。このステップＳ４の条件が成立すると、ステップＳ６に進み、アタッカからの攻撃と判断してサービス提供システム１０に通知する。

【００８５】またステップＳ５で、判断ルール２に従ったＩＤ情報が一致し生体情報の異なるものがあるか否かチェックする。このステップＳ５の条件が成立すると、ステップＳ６に進み、アタッカからの攻撃と判断してサービス提供システム１０に通知する。一方、ステップＳ４の判断ルール１の条件が成立し且つステップＳ５で判断ルール２の条件も成立しなかった場合には、ステップＳ７で正常利用と判断してシステムに通知する。

【００８６】本発明の不正アクセス判断システム１６からアタッカからの攻撃である旨の通知を受けたサービス提供システム１０は、そのとき入力しているＩＤ情報と生体情報と予め登録しているＩＤ情報の生体情報との間で照合一致が万が一得られていたとしても、例えばユーザ側に対し通常の認証以外の他のユーザ情報例えば生年月日等の入力を要求し、不正アクセスに対する防衛措置をとるようになる。

【００８７】また不正アクセス判断システム１６から通知された不正アクセスの内容が、例えば図６の不正アク

セス２５－３のように明らかにアタッカによる攻撃であることが分かっている場合には、ユーザに対し警告を発してサービス提供を拒否する。即ちサービス提供システム１０は、本発明による不正アクセス判断システム１６から不正アクセス者による認証請求である旨の通知を受けることで、不正アクセスの内容に対応した適切な防衛措置を迅速にとることができる。

【００８８】ステップＳ６又はステップＳ７に続くステップＳ８にあっては、ステップＳ１で生体情報入力記憶部１８及びＩＤ情報入力記憶部２０に一時的に入力記憶した生体情報とＩＤ情報を、利用情報記憶部２２に記憶して保存する。

【００８９】この場合、利用情報記憶部２２が一杯であれば、最も旧い保存ペアを証供してあらみたな入力ペアを記憶する。

【００９０】図８は、本発明の不正アクセス判断装置の第２実施形態のブロック図である。この第２実施形態にあっては、図２の不正アクセス判断システム１６に更にログ記録部３４を設けたことを特徴とする。それ以外の構成は図２の実施形態と同じである。

【００９１】ログ記録部３４には、制御部２８でアタッカからの攻撃による不正アクセスと判断された場合に、不正アクセス者の身元に関する情報を記録する。ログ記録部３４に記録する情報としては

①不正アクセス時の生体情報

②不正アクセスの入力時刻

③不正アクセスの電話番号もしくはネットワークアドレス

④不正アクセスの対象となったＩＤ情報

等を記録する。ここで、不正アクセスを行ったユーザ端末の電話番号もしくはネットワークアドレスは、サービス提供システム１０に設けているネットワーク通信部の例えばプロトコル層から収集することが可能である。

【００９２】図９は、図８の第２実施形態における不正アクセス判断処理のフローチャートである。図９において、ステップＳ１～Ｓ６の生体情報とＩＤ情報の入力記憶に対する保存情報との比較照合による不正アクセスの判断は、図７のフローチャートと同じであるが、ステップＳ６でアタッカからの攻撃と判断してサービス提供システム１０に通知した後にステップＳ７で不正アクセスと判断されたとき、入力記憶した生体情報と時間を例えばログ記憶部３４に記憶している。

【００９３】このように図８の第２実施形態にあっては、ログ記録部３４に不正アクセスと判断されたときの生体情報や時刻等を記録してアタッカ自身の身元情報を残しておくことにより、後の犯罪捜査でアタッカがだれであるかを証明すること等が可能となる。

【００９４】図１０は、本発明の不正アクセス判断装置の第３実施形態のブロック図である。この第３実施形態にあっては、図８の第２実施形態の不正アクセス判断システム１６に、更に時計部３６と電子メール発行部３８を設けたことを特徴とし、それ以外の構成は図２の実施形態と同じである。

【００９５】時計部３６は、時刻情報として「年、月、日、時、分」を計測して保持し、この時刻情報を利用情報記憶部２２及び制御部２８に通知する。制御部２８は、時計部３６からの時刻情報に基づいて利用情報記憶部２２の保存内容を制御しており、記憶されてから所定時間を過ぎたＩＤ情報と生体情報の保存ペアを消去する。

【００９６】この結果、利用情報記憶部２２には、入力してから一定時間内の過去に入力したＩＤ情報と生体情報のペアのみが保存記憶されていることとなり、ユーザ端末１４からの認証請求に伴うサービス提供システム１０からの生体情報及びＩＤ情報の入力を受けた際の生体情報照合部２４及びＩＤ情報比較部２６による過去の保存情報との照合比較の数を制限でき、不正アクセス判断システム１６における判断処理の負担を軽減することができる。

【００９７】このように利用情報記憶部２２に保存記憶する過去に入力したＩＤ情報と生体情報のペアを制限しても、通常、アタッカからの攻撃は短時間に連続して行われることが多いことから、アタッカによる不正アクセスを判断する上で支障は起きない。

【００９８】更に図１０の第３実施形態にあっては、電子メール発行部３８を設けたことで、制御部２８は、アタッカからの攻撃による不正アクセスと判断した場合、アタッカによる不正アクセスがあった事実を電子メール発行部３８に通知する。

【００９９】電子メール発行部３８は、サービス提供システム１０がアタッカに攻撃された事実を知らせる電子メールを作成し、メールシステム４０に作成した電子メールを投函し、ＬＡＮやＷＡＮ等のネットワークを経由してシステム管理者端末４４に電子メールを送信する。これによってシステム管理者は、サービス提供システム１０に対しアタッカによる攻撃があったことを直ちに知ることができる。

【０１００】このためシステム管理者４４は、サービス提供システム１０のログをチェックするなどして常に不正アクセスに対するシステムの状態を監視する必要がなくなり、システム管理者の負担を大幅に軽減し、且つアタッカの攻撃に対しシステム管理者は直ちに適切な対応策をとることができる。

【０１０１】図１１は、図１０の利用情報記憶部２２の記憶内容であり、ＩＤ情報記憶領域２２－１、生体情報記憶領域２２－２に加え、時刻情報記憶領域２２－３を設けており、時刻情報記憶領域２２－３には例えばアドレス「０００００ｈ」のように、「年、月、日、時、分」である９８０９１７０９３５が格納されている。

【０１０２】制御部２８は、このような利用情報記憶部

２２にＩＤ情報と生体情報のペアと共に記憶された時刻情報を利用して、記憶から所定時間を過ぎた保存ペアを消去する記憶制御を行っている。

【０１０３】例えば現在時刻をｔｎとし、このときアドレス「８０００ｈ」に保存記憶が行われたとすると、制御部２８は例えば所定時間Ｔ＝６０分を記憶保存時間として設定しており、現在時刻ｔｎより所定時間Ｔ＝６０分前がアドレス「０００１ｈ」の時刻ｔｎ－１の記憶内容であったとすると、それ以前のアドレス「０００ｈ」の時刻ｔｎ－２の記憶内容を消去する。

【０１０４】この結果、利用情報記憶部２２には現在時刻ｔｎからＴ＝６０分の間に記憶されたＩＤ情報と生体情報のペアが時刻情報と共に保存されるだけであり、利用情報記憶部２２の保存記憶量を不正アクセスに必要な適正量に制限し、入力した生体情報とＩＤ情報と、利用情報記憶部２２に保存記憶された生体情報とＩＤ情報との比較照合の処理負担を低減することができる。

【０１０５】図１２は、図１０の第３実施形態における不正アクセス判断処理のフローチャートである。図１２において、ステップＳ１～ステップＳ６までの入力記憶した生体情報とＩＤ情報を保存記憶した生体情報とＩＤ情報と比較照合して不正アクセスかどうか判断する処理は、図９の第２実施形態のフローチャートと同じである。

【０１０６】これに対し不正アクセスと判断してステップＳ６でサービス提供システム１０にアタッカからの攻撃である旨を通知した場合、ステップＳ７で制御部２８は電子メール発行部３８にアタッカに攻撃された事実を通知し、システム管理者４４に対し電子メールを発行する。

【０１０７】更に次のステップＳ９において、制御部２８は時計部３６から与えられた現在時刻の時刻情報と図１１のように利用情報記憶部２２に記憶している時刻情報を用いて、記憶されてから所定時間が経過した生体情報とＩＤ情報の保存ペアを消去する。

【０１０８】この保存記憶の消去が済んだ後、ステップＳ１０で、そのとき生体情報入力記憶部１８及びＩＤ情報入力記憶部２０に一時的に入力記憶している入力したＩＤ情報と生体情報のペアを、時計部３６から得られている時刻情報と共に利用情報記憶部２２に記憶して保存する。

【０１０９】図１３は、本発明の不正アクセス判断装置の第４実施形態のブロック図である。この第４実施形態にあっては、図１０の第３実施形態に対し更に、端末アドレス記憶部４８と同一端末アクセス検知部５０を設けている。また図１０の電子メール発行部３８に代えて、アラーム信号発行部５４を設けている。それ以外の点は図１０の第３実施形態と同じである。

【０１１０】端末アドレス記憶部４８は、サービス提供システム１０に対しユーザ端末１４よりＩＤ情報と生体情報のペアを使用した認証請求があった際に、認証請求を行ったユーザ端末１４の電話番号やネットワークアドレスを記憶する。

【０１１１】このユーザ端末１４が認証請求を行ったときの電話番号やネットワークアドレスは、サービス提供システム１０に設けているネットワーク通信部５２から得られる。具体的には、ネットワーク通信部５２のプロトコル層における受信パラメータとして電話番号やネットワークアドレスを取得することができる。

【０１１２】図１４は、図１３の端末アドレス記憶部４８の記憶内容を利用情報記憶部２２と共に示している。図１４の端末アドレス記憶部４８は、図６の不正アクセス２５－３のように、アタッカがＩＤ情報と生体情報の両方を変えながら攻撃した場合のアタッカが使用したユーザ端末の端末アドレスを時刻ｔ１～ｔ５について記憶したもので、同じ端末アドレスＡ１が記憶されている。

【０１１３】また利用情報記憶部２２には、図６の不正アクセス２５－３の時刻ｔ１～ｔ６の不正アクセスによるＩＤ情報と生体情報の入力ペアに対応した保存ペアが、時刻情報ｔ１～ｔ５と共に記憶されている。

【０１１４】再び図１３を参照するに、同一端末アクセス検知部５０は、端末アドレス記憶部４８を参照し、「所定時間内に同一端末位置から所定回数以上の認証請求がある」の条件が成立するか否か検知する。この条件成立を検知すると、制御部２８に対し不正アクセス判断のための処理要求を行う。

【０１１５】例えば図１４の端末アドレス記憶部４８を例にとると、同一端末アクセス検知部５０は新たな認証請求の入力時刻から過去所定時間Ｔ１、例えばＴ１＝１５分以内に、同一端末アドレスから所定回数Ｎ回以上例えばＮ＝５回以上の認証請求があったか否かチェックしている。

【０１１６】この場合、入力時刻ｔ５の時点で過去Ｔ１＝１５分以内に同じ端末アドレスＡ１より５回の認証請求があることから、このとき同一端末アクセス検知部５０は制御部２８に対し不正アクセスの判断処理を要求する。

【０１１７】このため制御部２８は、生体情報照合部２４及びＩＤ情報比較部２６を起動し、時刻ｔ５の入力ペア（ＩＤ２，ＬＢ２）を、それまでに記憶している保存ペアと比較照合する。この場合、利用情報記憶部２２に示している時刻ｔ１，ｔ２，ｔ３，ｔ４の保存ペアとの間で、図６の判断ルールが成立して不正アクセス者による認証請求であることが判断される。

【０１１８】ここで、同一端末アクセス検知部５０で同一端末からの認証請求の回数Ｎを判断するための一定時間Ｔ１は、アタッカによる攻撃が短時間に連続して行われることから、長くても３０分から１時間程度の時間で十分である。

【０１１９】また同一端末からのアクセス回数Ｎとして

はＮ＝５回を例にとっているが、正規のユーザによるＩＤ情報の入力ミスによるやり直しを何回許容するかによって、不正アクセスの処理要求を行う同一端末アクセスからのアクセス回数Ｎを決めればよい。例えば図１４の場合には、Ｎ＝５回で不正アクセスの判断要求を行っていることから、４回までは正規ユーザによるＩＤ情報の入力ミスによるやり直しを許容していることになる。

【０１２０】再び図１３を参照するに、アラーム信号発生部５４は制御部２８で不正アクセス者による認証請求と判断された場合、アタッカによる攻撃が行われた事実をシステム管理者に知らせるため、アラーム信号をネットワーク４２を経由してシステム管理者端末４４に通知してアラームを出させる。

【０１２１】更に、この場合、ログ記録部３２は制御部２８で不正アクセス者による認証請求と判断されたときの生体情報入力記憶部１８及びＩＤ情報入力記憶部２０に一時記憶されている生体情報及びＩＤ情報の他に、端末アドレス記憶部４８からユーザ端末の電話番号やネットワークアドレスを記録し、更に時計部３６からの時刻情報も記録する。

【０１２２】図１５は、図１３の第４実施形態による不正アクセス判断処理のフローチャートである。図１５において、ステップＳ１でサービス提供システム１０がユーザ端末１４から受信した生体情報とＩＤ情報を取得して、生体情報入力記憶部１８及びＩＤ情報入力記憶部２０にそれぞれ入力記憶し、更に端末アドレス記憶部４８にそのときネットワーク通信部５２から得られた例えばユーザ端末１４のネットワークアドレスを記録する。

【０１２３】次にステップＳ２で、同一端末アクセス検知部５０が端末アドレス記憶部４８を参照し、同一端末から所定時間内に所定回数以上の利用要求即ち認証請求があったか否かチェックする。このステップＳ２の条件が得られると、ステップＳ３～Ｓ７，Ｓ９のように、図３の実施形態と同様な不正アクセスの判断処理が行われる。

【０１２４】そしてステップＳ７で不正アクセス者の認証請求を判断してサービス提供システムにアタッカからの攻撃を通知した後、ステップＳ８でアラーム信号発生部５４からシステム管理者４４にアラーム信号を発行し、サービス提供システム１０に対しアタッカから攻撃があったことを知らせる。

【０１２５】続いてステップＳ１０で利用情報記憶部２２の記憶から一定時間過ぎた保存内容を消去した後、ステップＳ１１で、このとき入力記憶した生体情報とＩＤ情報のペアを時刻情報と共に記憶して、このときの認証請求に伴う一連の処理を終了する。

【０１２６】次に本発明の不正アクセス判断システム１６の制御部２８において、不正アクセスを判断するための判断ルール４，５，６を説明する。

【０１２７】図１６の不正アクセスの判断処理は、判断ルール４を使用した場合である。判断ルール４は、同一端末について新たに入力したＩＤ情報と過去の所定時間内に入力したＩＤ情報とを比較した結果が不一致の場合、不正アクセス者による認証請求と判断する。

【０１２８】この判断ルール４の特徴は、生体情報の照合を行っていない点である。このように生体情報の照合を行わずにＩＤ情報から不正アクセスを判断することで、不正アクセス判断処理の負担を大幅に減らすことができる。

【０１２９】アタッカによる攻撃の中には、図４の不正アクセス２５－１に示したように、特定のユーザ端末から生体情報を変えずにＩＤ情報を変えながら連続的に攻撃するパターンがある。この図４の不正アクセス２５－１のような攻撃パターンについては、生体情報は同じであることから、過去に入力した生体情報と比較せず、ＩＤ情報の変化のみを捉えることで、アタッカによる攻撃と判断することができる。

【０１３０】この図１６に適用される判断ルール４は、図１３の第４実施形態のように、端末アドレス記憶部４８に認証請求を行ったユーザ端末の電話番号やネットワークアドレス等が記憶されている場合に有効である。

【０１３１】図１６の判断ルール４を適用した不正アクセス判断処理を説明すると次のようになる。まずステップＳ１で、サービス提供システム１０が受信した生体情報とＩＤ情報を取得して生体情報入力記憶部１８及びＩＤ情報入力記憶部２０に記憶し、更にネットワーク通信部５２から端末アドレス例えばネットワークアドレスを取得して端末アドレス記憶部４８に記憶する。

【０１３２】次にステップＳ２で同一端末から所定時間内に送られたＩＤ情報同士を照合する。この場合、図１４のように、端末アドレス記憶部４８において、例えば現在時刻ｔ５を基準に所定時間Ｔ＝１５分前までの同一端末アドレスＡ１に対応する利用情報記憶部２２のＩＤ情報を参照する。

【０１３３】このときのアタックは図４の不正アクセス２５－１のようなパターンを想定していることから、同一端末アドレスＡ１の所定時間Ｔ１で利用情報記憶部２２から得られるＩＤ情報はＩＤ１，ＩＤ２，ＩＤ３，ＩＤ４，・・・というように異なっている。

【０１３４】そこでステップＳ３でＩＤ情報が不一致か否かチェックし、不一致であればステップＳ４に進み、アタッカからの攻撃と判断してサービス提供システム１０に通知する。それ以降の処理は図１５のステップＳ８，９以降と同じである。

【０１３５】図１７は、例えば図１４の第４実施形態の制御部２８に判断ルール５を適用した場合の不正アクセス判断処理のフローチャートである。

【０１３６】判断ルール５は、入力したＩＤ情報に対し過去のＩＤ情報が連番となっているか否か判定し、連番を判定した際には所定回数まで不正アクセス者による認

証請求と判断する。

【０１３７】新たなＩＤ情報の入力記憶を受けた際に、過去に入力したＩＤ情報を参照して連番となっている場合には、一層アタッカからの攻撃である可能性が高い。これはアタッカがコンピュータを使用してＩＤ番号を順番に変えながら攻撃していることが考えられるからである。したがって、判断ルール５によって入力されるＩＤ番号が連番であるかどうかを調べるとアタッカからの攻撃であることの確信が持て、これによって不正アクセスかどうかの確からしさが更に向上する。

【０１３８】図１７の判断ルール５を適用した不正アクセス判断処理を説明すると次のようになる。まずステップＳ１でサービス提供システム１０が受信した生体情報とＩＤ情報を取得して入力記憶する。次にステップＳ２で、入力記憶したＩＤ情報と利用情報記憶部２２に保存記憶している過去に連続入力した所定数のＩＤ情報を比較する。

【０１３９】ステップＳ３でＩＤ情報が連番か否かチェックし、連番であれば、ステップＳ４で不正アクセス者によるアタッカからの認証請求による攻撃と判断し、サービス提供システム１０に通知する。ステップＳ５以降は図１６と同じである。

【０１４０】図１８は、図１３の第４実施形態の制御部２８の不正アクセスの判断に適用される判断ルール６を用いたフローチャートである。

【０１４１】判断ルール６は、入力した生体情報と過去に入力した生体情報が一致した際に、生体情報が一致しＩＤ情報が異なるそれ以外の組合せを検出し、この組合せ数が所定数に達したときに不正アクセス者による認証請求と判断する。

【０１４２】この判断ルール６は、図４に示した判断ルール１の変形と言える。即ち図４の判断ルール１にあっては、生体情報が一致しＩＤ情報が不一致とする条件が１つでも成立すると不正アクセス者による認証請求と判断している。これに対し判断ルール６は、判断ルール１の条件が所定数以上となったときに不正アクセス者による認証請求と判断する。

【０１４３】この判断ルール６は、アタッカが不正にアクセスしようとしたのではなく、正規のユーザが単にＩＤ情報を入力し間違えた場合に、誤って不正アクセス者による認証請求と判断してしまうことを回避するためである。

【０１４４】具体的には、図４の不正アクセス２５－１がアタッカによるものではなく正規のユーザがＩＤ情報の入力ミスをして、やり直した場合であるとする。この場合、例えば不正アクセスと判断するＩＤ番号の相違回数をＮ回に設定していたとすると、正規ユーザはＮ＋１回までＩＤ情報の入力ミスが許容される。例えば不正アクセスと判断するＩＤ情報の不一致数をＮ＝３回に設定していたとすると、正規ユーザはＮ＋１＝４回の入力ミスが許容できる。

【０１４５】このため図４の不正アクセス２５－１のように、ユーザが４回連続してＩＤ情報の入力ミスを行ったとすると、これに対応した利用情報記憶部２２の保存記憶からＩＤ情報の不一致数は時刻ｔ１では０回、時刻ｔ２では１回、時刻ｔ３では２回、時刻ｔ４では３回であり、この時点まで正規ユーザの入力ミスが許容される。　もう１回ＩＤ情報の入力を誤ると、そのときの利用情報記憶部２２の保存ＩＤ情報に基づく不一致数は４回となり、この時点で不正アクセス者による認証請求と判断される。

【０１４６】この判断ルール６を適用した不正アクセス判断処理を図１８のフローチャートについて説明すると、次のようになる。まずステップＳ１でサービス提供システム１０が受信したユーザの認証請求に伴う生体情報とＩＤ情報を取得して入力記憶し、ステップＳ２で、入力記憶した生体情報と過去の全ての生体情報を照合し、ステップＳ３で生体情報が一致しＩＤ情報が異なるものがあるか否かチェックする。

【０１４７】この条件を満足するものがあればステップＳ４に進み、該当する組合せは予め定めたＮ個以上か否かチェックする。Ｎ個未満であれば正規ユーザによるＩＤ情報の間違いによる再入力と判断し、ステップＳ７で正常利用と判断してシステムに通知する。

【０１４８】Ｎ個以上であった場合にはステップＳ５に進み、アタッカからの攻撃と判断してサービス提供システムに通知し、更にステップＳ６でシステム管理者にアラーム信号を発行する。ステップＳ８，Ｓ９は図１７のステップＳ７，Ｓ８と同じである。

【０１４９】尚、上記の実施形態は、制御部における不正アクセスの判断に判断ルール１～６を個別に適用する場合を例にとっているが、これらの判断ルールを適宜に組み合わせて不正アクセスを判断するようにしてもよい。

【０１５０】また上記の実施形態は、生体情報として指紋を例にとるものであったが、これ以外の生体情報である声紋、虹彩パターン、網膜血管パターン、掌形、耳形、顔等の各個人特有の生体情報についても全く同様に不正アクセスを判断することができる。

【０１５１】更に本発明は、その目的と利点を損なわない範囲の適宜の変形を全て含む。更にまた本発明は、上記の実施形態で示した数値による限定は受けない。

【０１５２】

【発明の効果】以上説明してきたように本発明によれば、サービス提供システムに入力される認証請求のための利用者のＩＤ番号と生体情報のペアについて、過去に入力されたＩＤ情報と生体情報の保存ペアと比べることで、アタッカによる不正アクセスの攻撃が行われているかどうかを推測判断し、アタッカからの攻撃の可能性があると判断した場合には、攻撃対象となっているサービ

ス提供システムにアタッカからの攻撃が行われていることを通知して適切な防衛対策をとらせることができる。

【０１５３】また生体情報は個人固有のものなので、不正アクセスと判断した際に、アタッカの身元情報をロギングしていくことで、次のアタッカの攻撃に対する対抗措置や後の犯罪捜査での有効な手掛かりを与えることができ、多数のユーザからのアクセスに対しサービスを提供するシステムのセキュリティを大幅に高めることができる。

【０１５４】尚、本発明の不正アクセス判断装置に於いて、その制御部は、不正アクセス者による認証請求を判断した際に、サービス提供システムの管理者に判断結果を自動通知することを特徴とする。

【０１５５】また本発明の不正アクセス判断方法に於いて、その制御過程は、不正アクセス者による認証請求を判断した際に、サービス提供システムの管理者に判断結果を自動通知することを特徴とする。

【図面の簡単な説明】

【図１】本発明の原理説明図

【図２】認証請求の入力情報と過去の入力記憶の全てを比較照合して不正アクセスを判断する本発明の第１実施形態のブロック図

【図３】固定記憶容量をもつ図２の利用情報記憶部の説明図

【図４】生体情報を固定しＩＤ情報を変えた判断ルール１が適用される不正アクセスと利用情報記憶部の説明図

【図５】ＩＤ情報を固定し生体情報を変えた判断ルール２が適用される不正アクセスと利用情報記憶部の説明図

【図６】ＩＤ情報と生体情報の両方を変えた判断ルール３が適用される不正アクセスと利用情報記憶部の説明図

【図７】図２の不正アクセス判断処理のフローチャート

【図８】不正アクセス者の身元情報を記憶するロギング機能を備えた本発明の第２実施形態のブロック図

【図９】図８の不正アクセス判断処理のフローチャート

【図１０】時間計測機能とシステム管理者への自動通報機能を備えた本発明の第３実施形態のブロック図

【図１１】図１０の利用情報記憶部の説明図

【図１２】図１０の不正アクセス判断処理のフローチャート

【図１３】端末アドレスの記憶機能を備えた本発明の第３実施形態のブロック図

【図１４】図１３の端末アドレス記憶部と利用情報記憶部の説明図

【図１５】同一端末から所定時間内に所定回数の認証請求があったときに起動する図１４の不正アクセス判断処理のフローチャート

【図１６】同一端末から所定時間内に入力したＩＤ情報のみにより不正アクセスを判断する判断ルール４が適用される図１４の不正アクセス判断処理のフローチャート

【図１７】ＩＤ情報の連番入力から不正アクセスを判断する判断ルール５が適用される図１４の不正アクセス判断処理のフローチャート

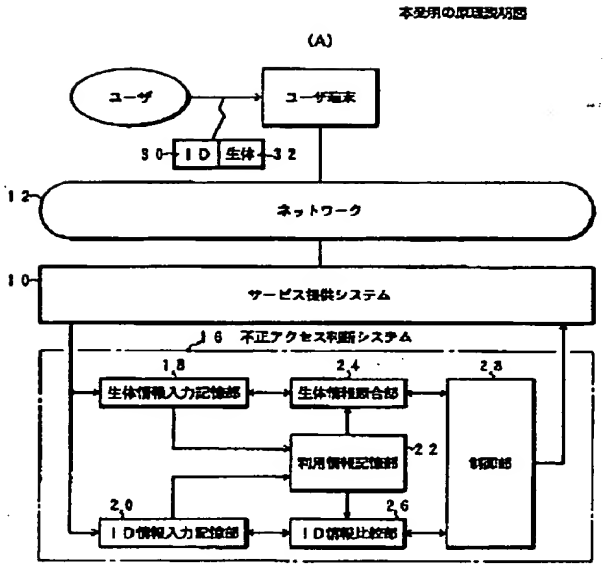
【図１８】ＩＤ情報につき正規ユーザによる誤入力と不正アクセスによる入力を区別する判断ルール６が適用される図１４の不正アクセス判断処理のフローチャート

【符号の説明】

１０：サービス提供システム
１２，４２：ネットワーク（ＬＡＮ／ＷＡＮ）
１４：ユーザ端末
１６：不正アクセス判断システム
１８：生体情報入力記憶部
２０：ＩＤ情報入力記憶部
２２：利用情報記憶部
２４：生体情報照合部
２５－１：不正アクセス（アタック１）
２５－２：不正アクセス（アタック２）
２５－３：不正アクセス（アタック３）
２６：ＩＤ情報比較部
２８：制御部
３０：ＩＤ情報
３２：生体情報
３４：ログ記憶部
３６：時計部
３８：電子メール発行部
４２：メールシステム
４４：システム管理者
４６：時刻情報
４８：端末アドレス記憶部
５０：同一端末アクセス検知部
５２：ネットワーク通信部

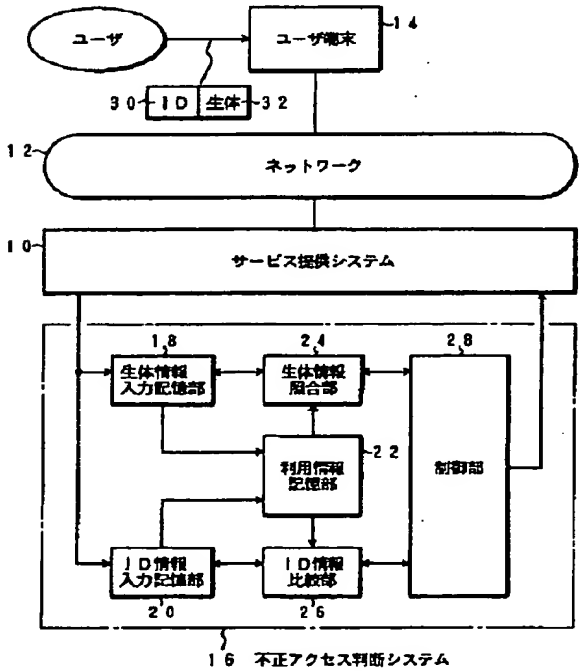
【図１】

本発明の原理説明図



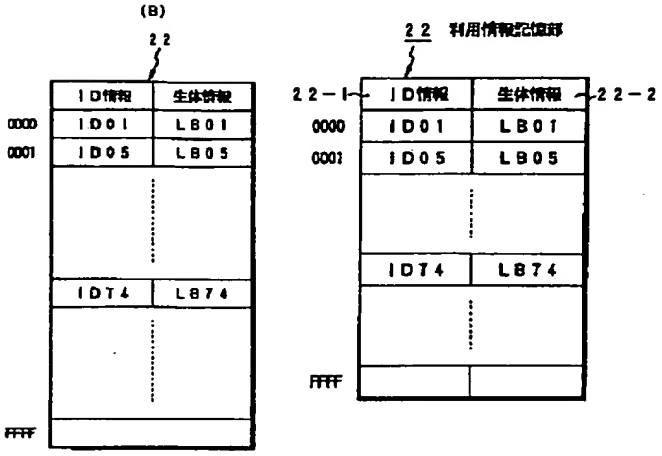
【図２】

認証請求の入力情報と過去の入力記憶の全てを比較照合して不正アクセスを判断する本発明の第１実施形態のブロック図



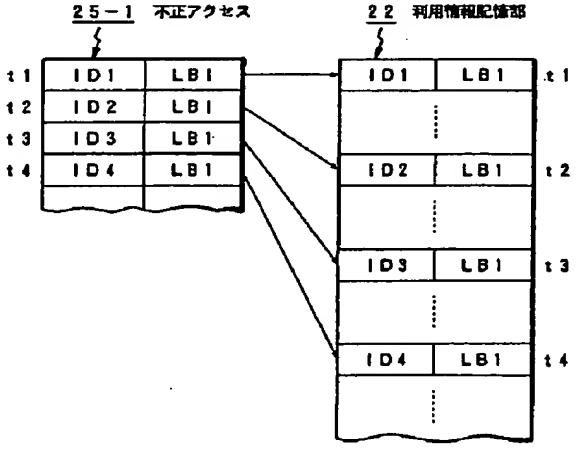
【図３】

固定記憶容量をもつ図２の利用情報記憶部の説明図



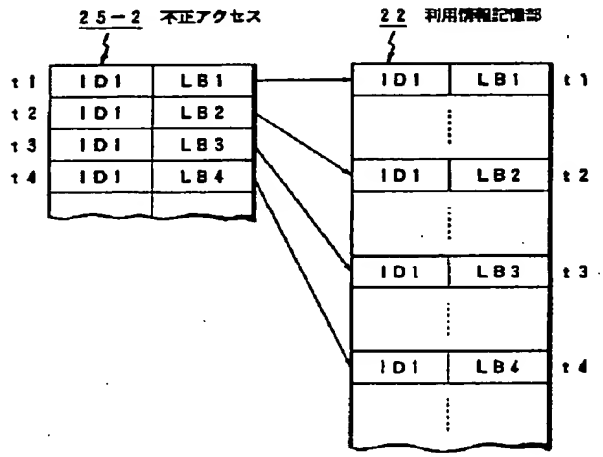
【図４】

生体情報を固定しＩＤ情報を変えた判断ルール１が適用される不正アクセスと利用情報記憶部の説明図



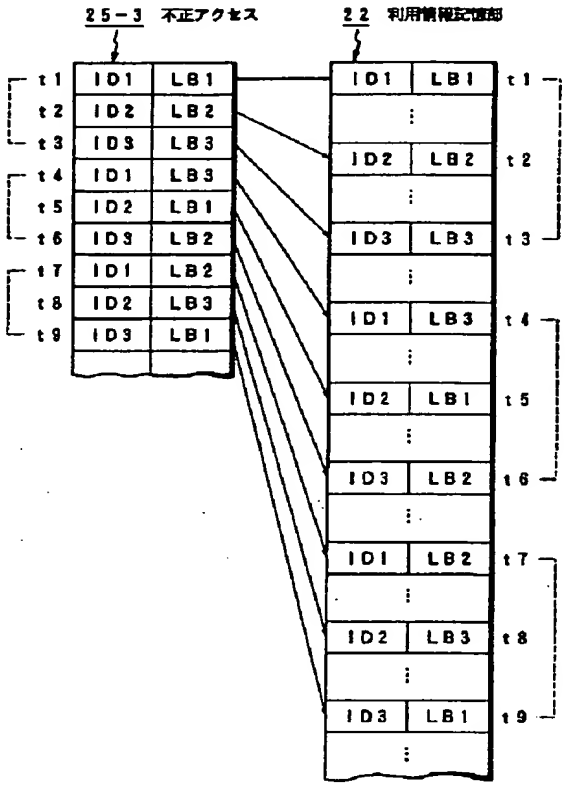
【図５】

ＩＤ情報を固定し生体情報を変えた判断ルール２が適用される不正アクセスと利用情報記憶部の説明図



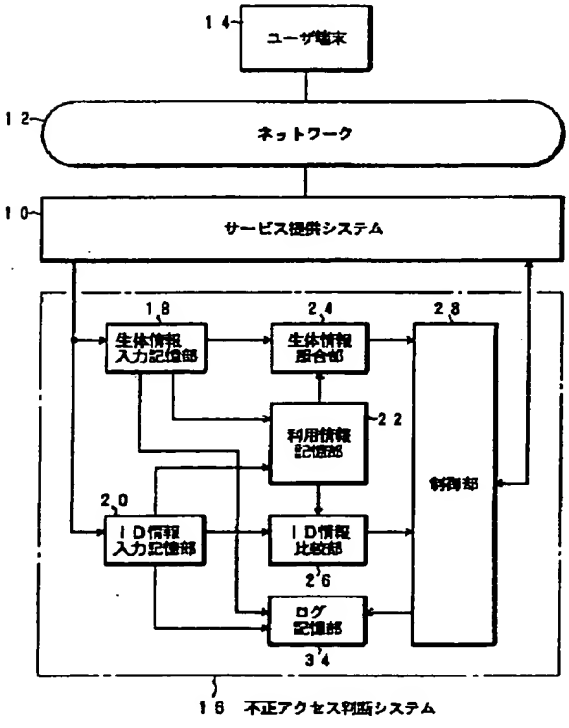
【図６】

ＩＤ情報と生体情報の両方を変えた判断ルール３が適用される不正アクセスと利用情報記憶部の説明図



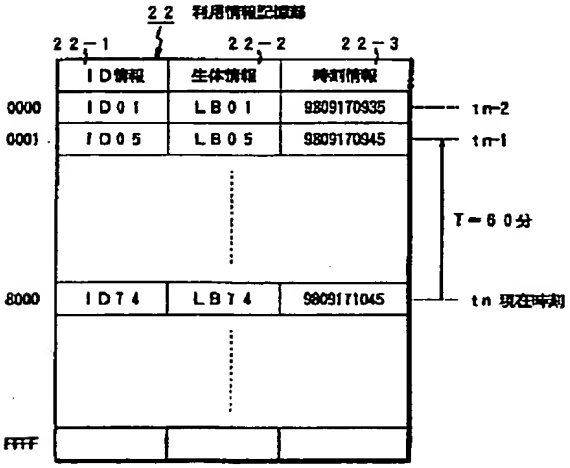
【図８】

不正アクセス者の身元情報を記憶するロギング機能を備えた本発明の第２実施形態のブロック図



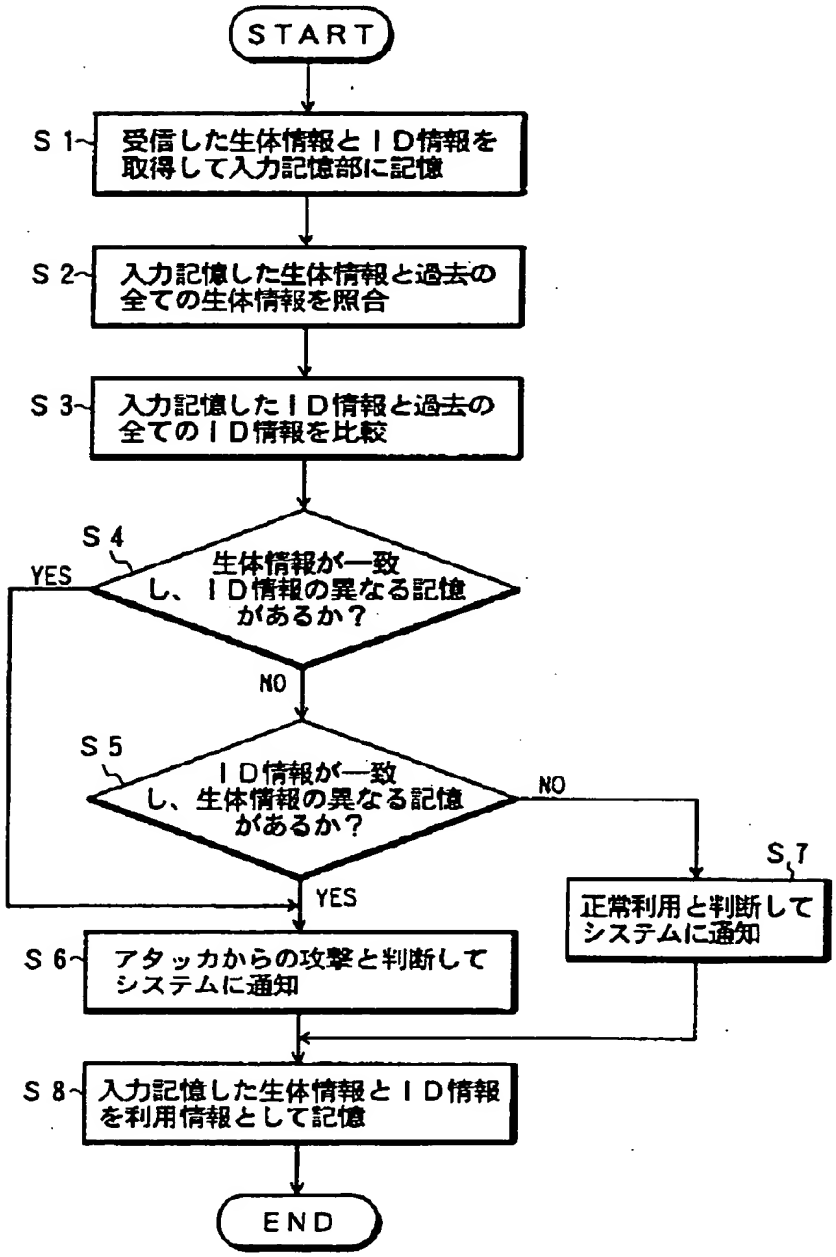
【図１１】

図１０の利用情報記憶部の説明図



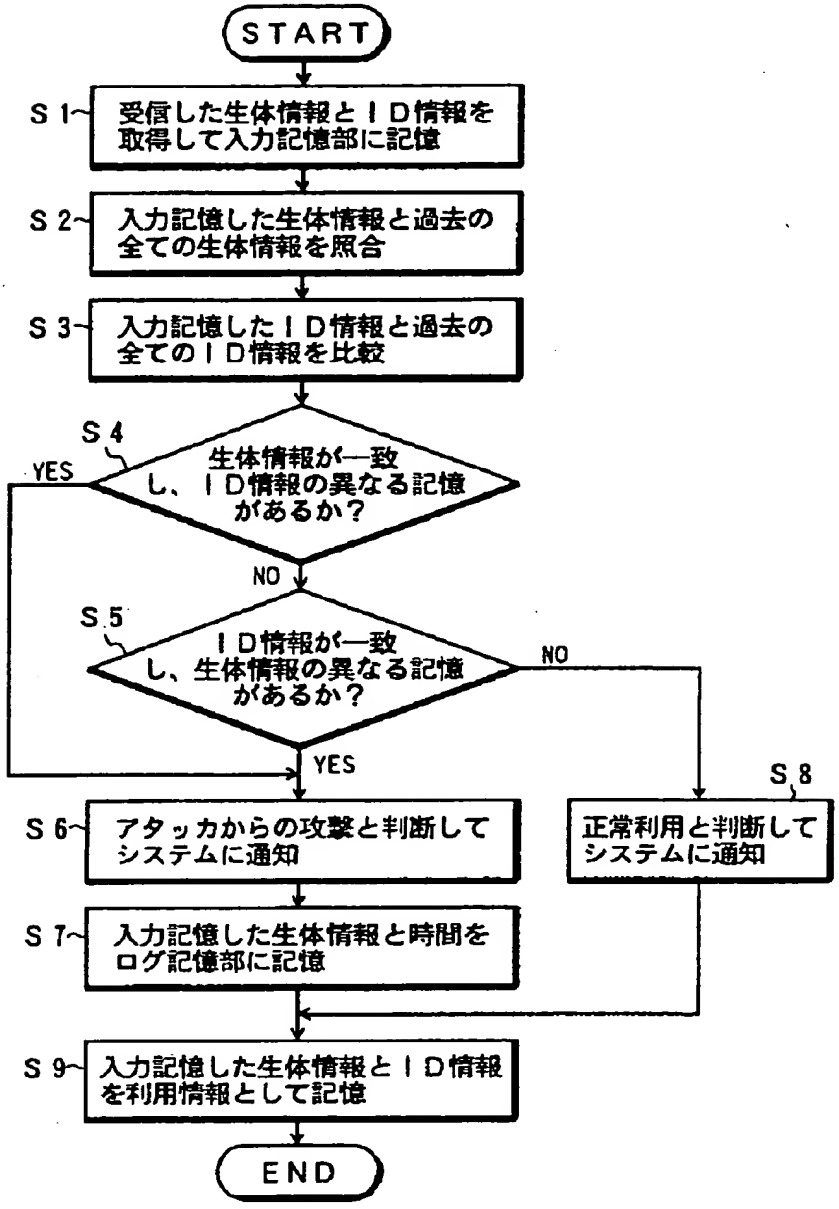
【図７】

図２の不正アクセス判断処理のフローチャート



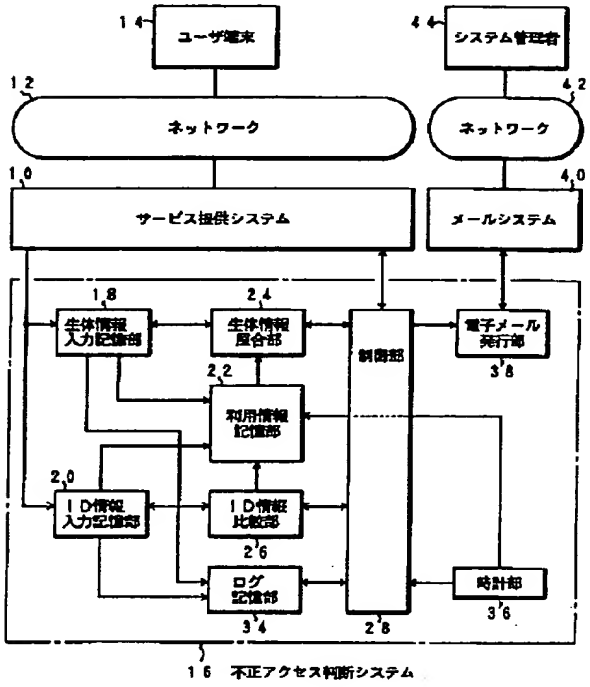
【図９】

図８の不正アクセス判断処理のフローチャート



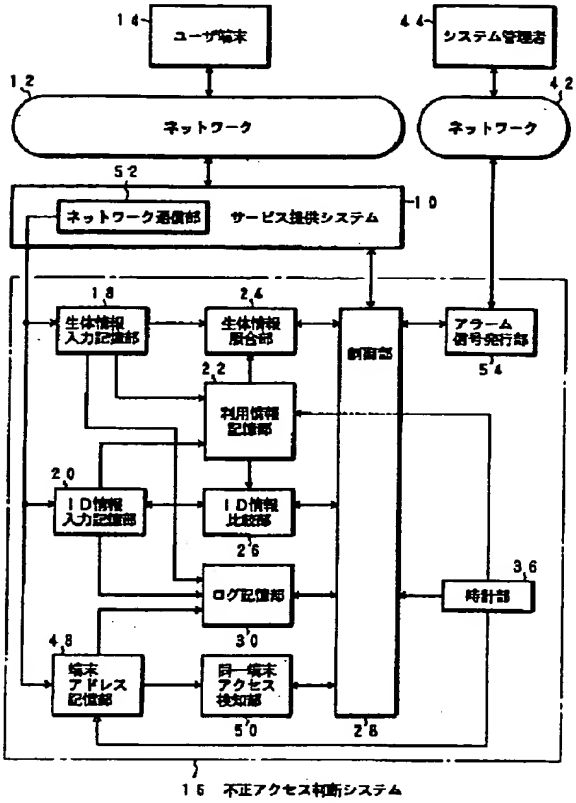
【図１０】

時間計測機能とシステム管理者への自動通報機能を備えた本発明の第３実施形態のブロック図



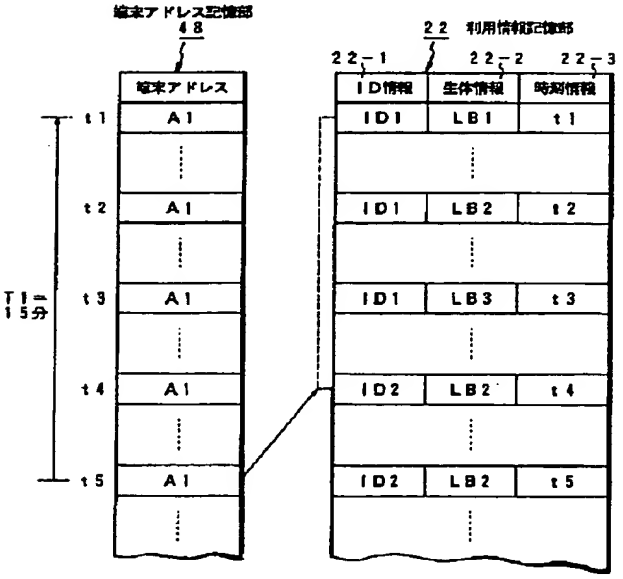
【図１３】

端末アドレスの記憶機能を備えた本発明の第３実施形態のブロック図



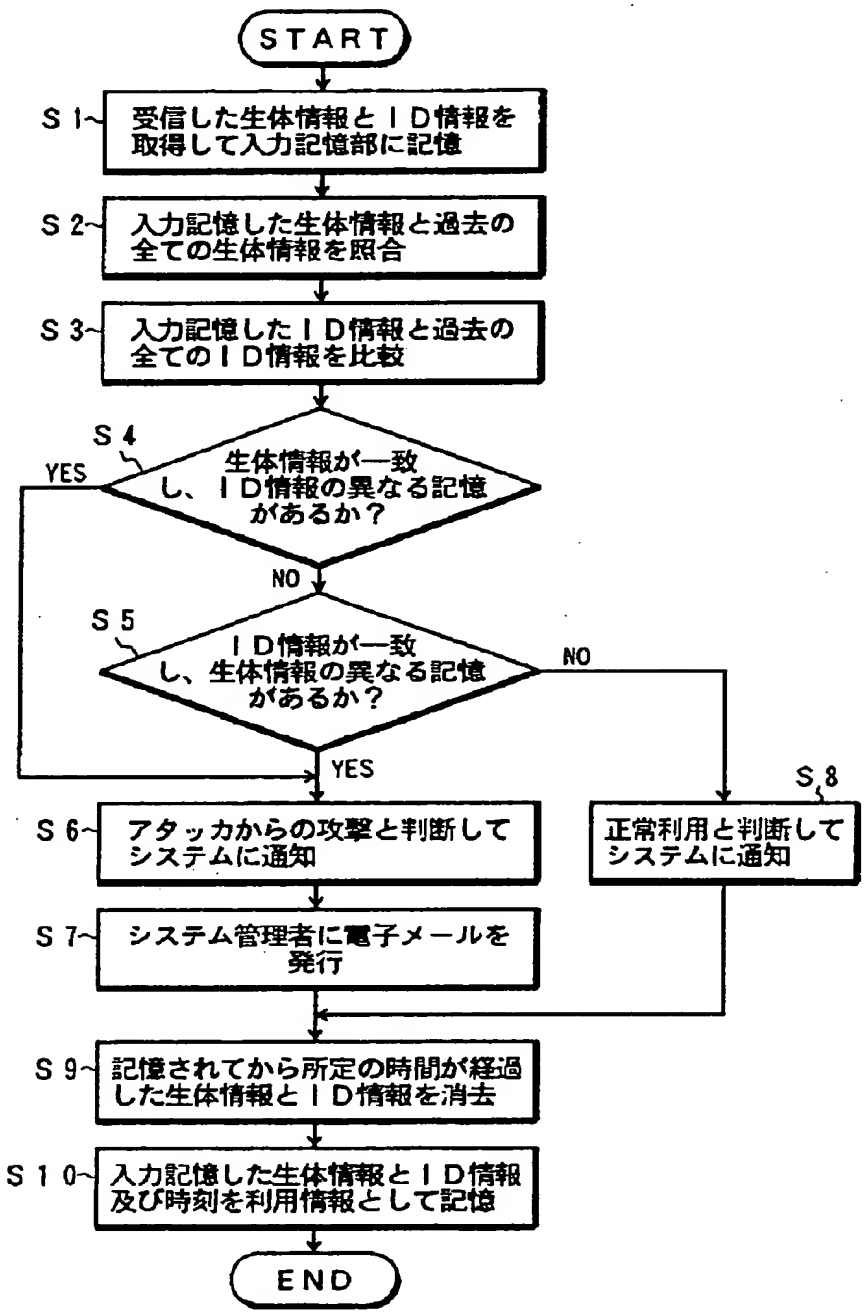
【図１４】

図１３の端末アドレス記憶部と利用情報記憶部の説明図



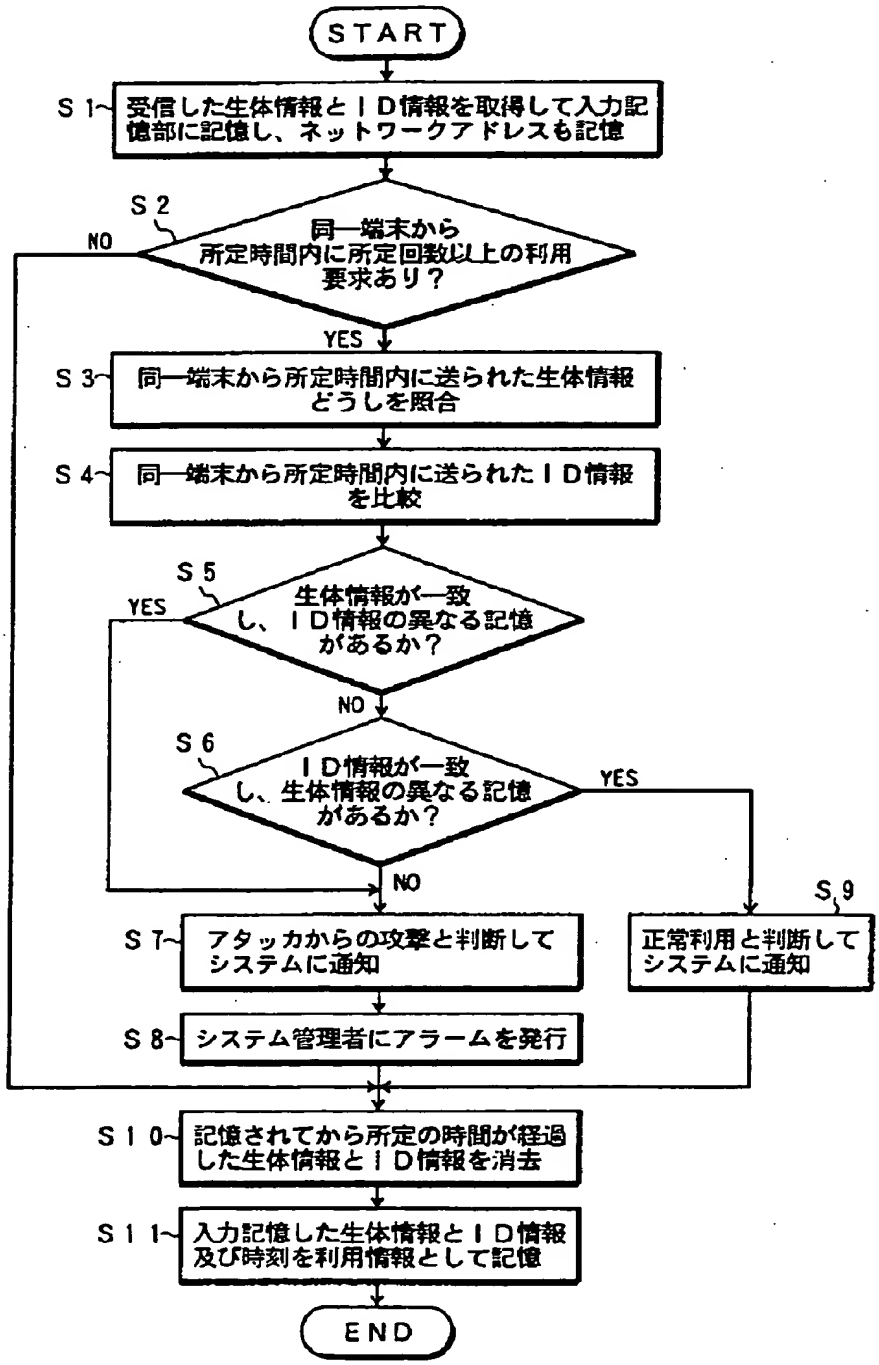
【図１２】

図１０の不正アクセス判断処理のフローチャート



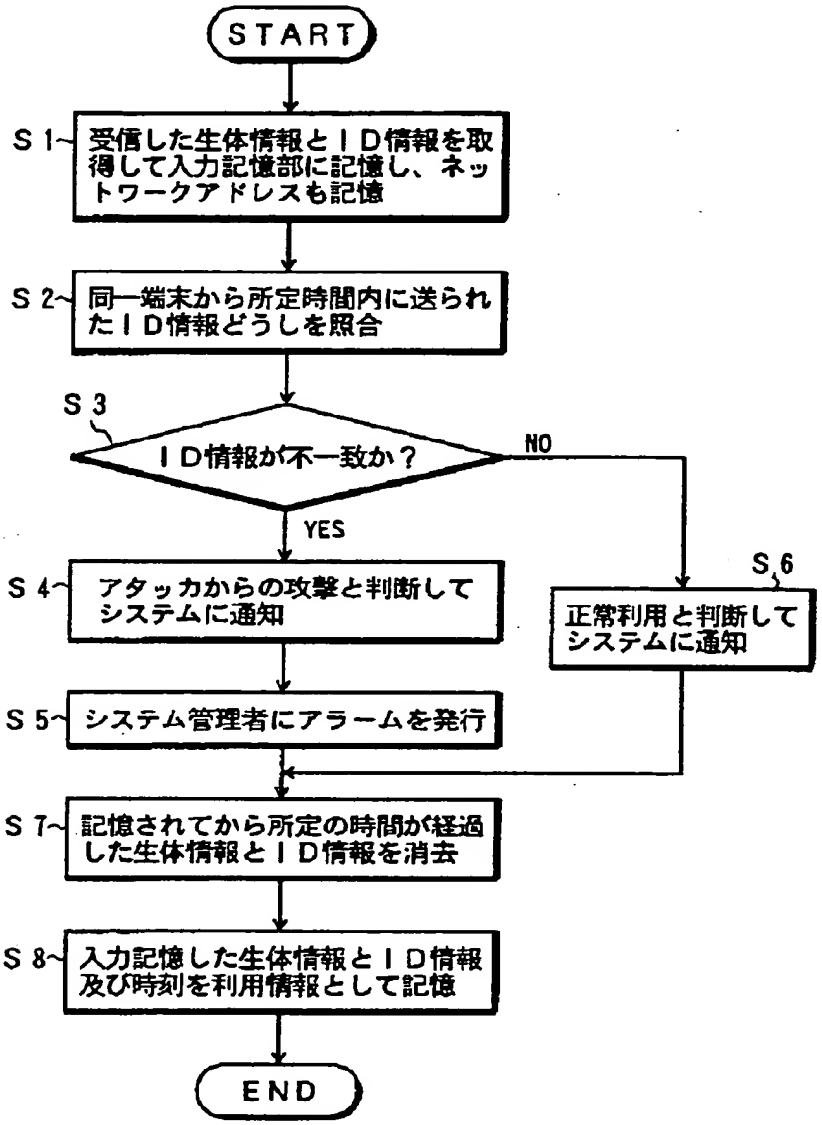
【図１５】

同一端末から所定時間内に所定回数の認証請求があったときに起動する図１４の不正アクセス判断処理のフローチャート



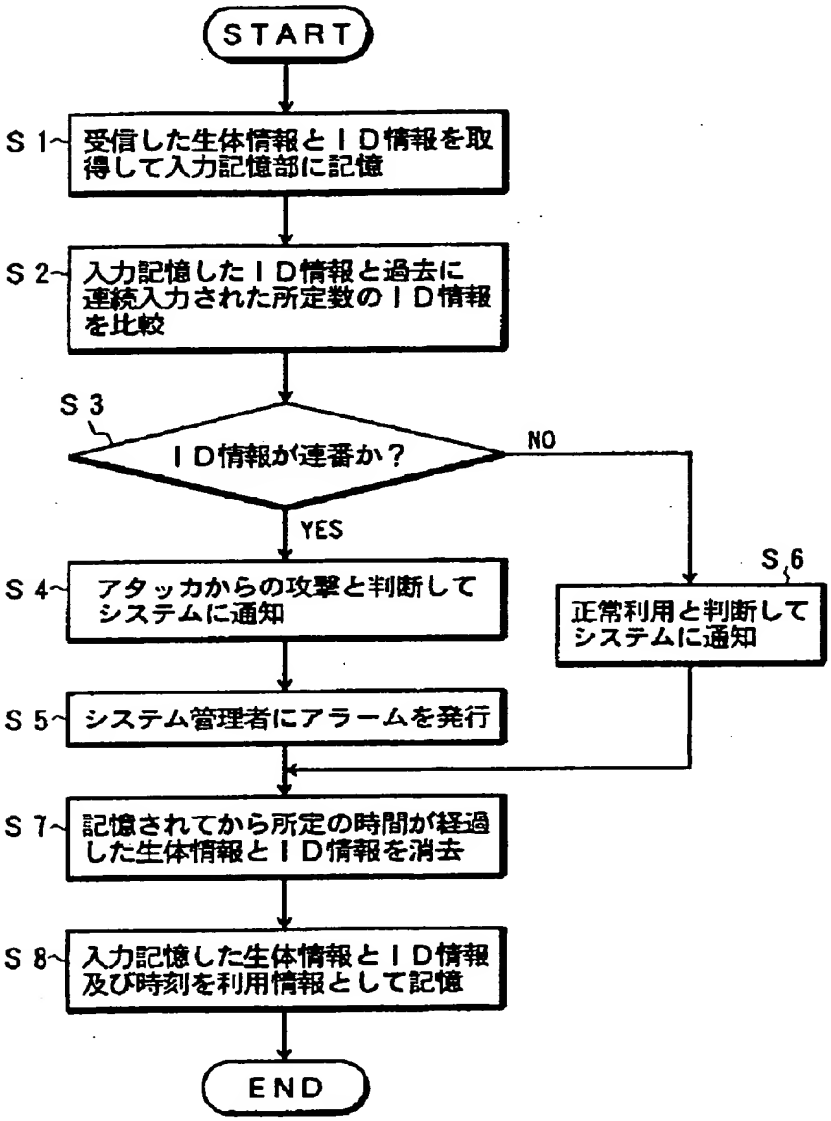
【図１６】

同一端末から所定時間内に入力したＩＤ情報のみにより不正アクセスを判断する判断ルール４が適用される図１４の不正アクセス判断処理のフローチャート



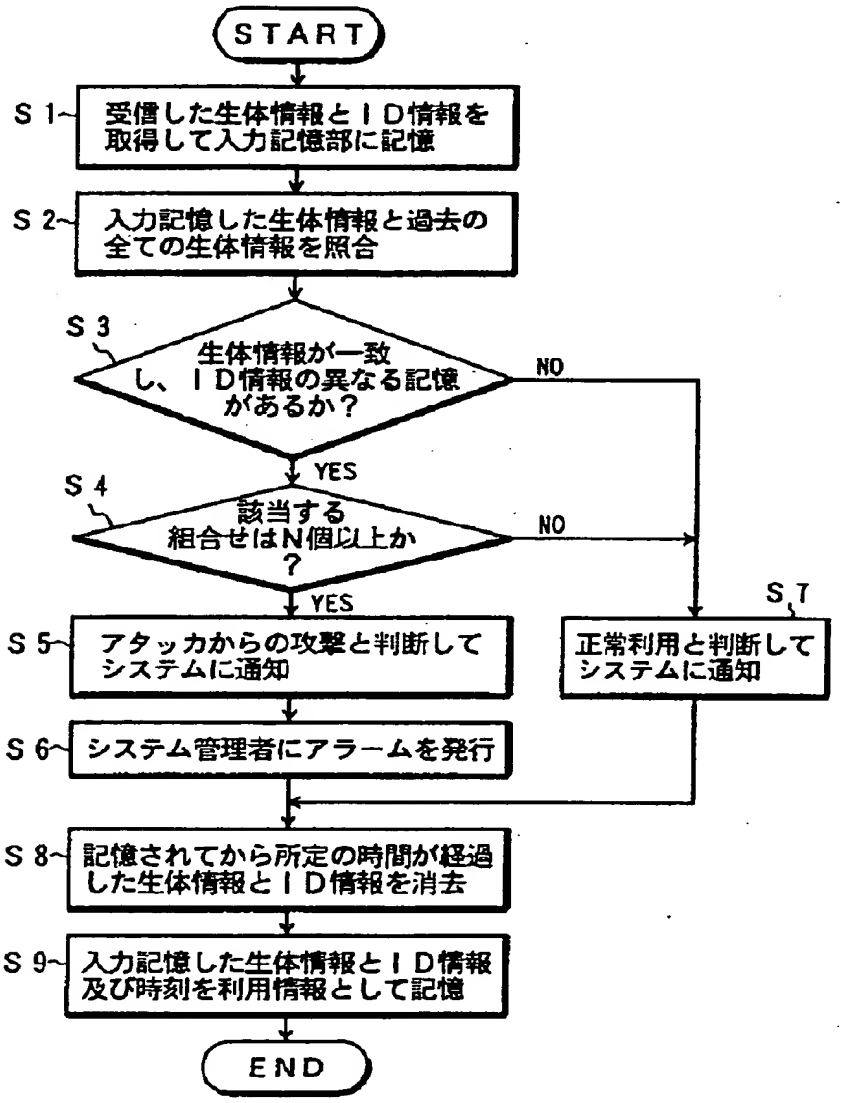
【図１７】

ＩＤ情報の連番入力から不正アクセスを判断する判断ルール５が適用される図１４の不正アクセス判断処理のフローチャート



【図１８】

ＩＤ情報につき正規ユーザによる誤入力と不正アクセスによる入力を区別する判断ルール６が適用される図１４の不正アクセス判断処理のフローチャート



【手続補正書】
【提出日】平成１１年１０月２５日（１９９９．１０．２５）
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】０００５
【補正方法】変更
【補正内容】
【０００５】そこでシステムを利用するための認証請求に対する本人確認のため、ＩＤコードに諮問や虹彩などの生体情報を組み合わせてセキュリティを高めているが、正規ユーザの生体情報を不正に入手できれば、ＩＤコードを変えながら生体情報を連続入力するといった手法でアタックされる可能性がある。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００３３
【補正方法】変更
【補正内容】

【００３３】ＩＤ情報に比べ生体情報は、盗むことが困難であることを考えると、用いられた生体情報はアタッカのものである確率が高く、これをロギングすることで犯罪捜査の手掛かりとでき、不正アクセス者の特定や証拠に活用できる。

【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】００８９
【補正方法】変更
【補正内容】
【００８９】この場合、利用情報記憶部２２が一杯であれば、最も旧い保存ペアを証供して新たな入力ペアを記憶する。

【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】００９２
【補正方法】変更
【補正内容】
【００９２】図９は、図８の第２実施形態における不正アクセス判断処理のフローチャートである。図９において、ステップＳ１～Ｓ６の生体情報とＩＤ情報の入力記憶に対する保存情報との比較照合による不正アクセスの判断は、図７のフローチャートと同じであるが、ステップＳ６でアタッカからの攻撃と判断してサービス提供システム１０に通知した後にステップＳ７で不正アクセスと判断されたとき、入力記憶した生体情報と時間を例えばログ記録部３４に記憶している。

【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】００９９
【補正方法】変更
【補正内容】
【００９９】電子メール発行部３８は、サービス提供システム１０がアタッカに攻撃された事実を知らせる電子メールを作成し、メールシステム４０に作成した電子メールを投函し、ＬＡＮやＷＡＮ等のネットワークを経由してシステム管理者４４に電子メールを送信する。これによってシステム管理者は、サービス提供システム１０に対しアタッカによる攻撃があったことを直ちに知ることができる。

【手続補正６】
【補正対象書類名】明細書
【補正対象項目名】０１２０
【補正方法】変更
【補正内容】
【０１２０】再び図１３を参照するに、アラーム信号発生部５４は制御部２８で不正アクセス者による認証請求と判断された場合、アタッカによる攻撃が行われた事実をシステム管理者に知らせるため、アラーム信号をネットワーク４２を経由してシステム管理者４４に通知してアラームを出させる。

フロントページの続き

Ｆターム(参考) 5B043 BA02 BA04 CA09 FA02 GA18
HA20
5B085 AE02 AE25 AE26